

# Distinguishability Measures and Entropies for General Probabilistic Theories

Gen Kimura <sup>[a],\*</sup> Koji Nuida <sup>[a],†</sup> and Hideki Imai <sup>[a],[b]</sup>

<sup>[a]</sup> *Research Center for Information Security (RCIS),  
National Institute of Advanced Industrial Science and Technology (AIST). Daibiru building 1003,  
1-18-13 Sotokanda, Chiyoda-ku, Tokyo, 101-0021, Japan*

<sup>[b]</sup> *Graduate School of Science and Engineering,  
Chuo University. 1-13-27 Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan*

As a part of the construction of an information theory based on general probabilistic theories, we propose and investigate the several distinguishability measures and “entropies” in general probabilistic theories. As their applications, no-cloning theorems, information-disturbance theorems are reformulated, and a bound of the accessible informations is discussed in any general probabilistic theories, not resorting to quantum theory. We also propose the principle of equality for pure states which makes general probabilistic theories to be more realistic, and discuss the role of entropies as a measure of pureness.

## I. INTRODUCTION

Recent development of the quantum information theory has shown us the ability of information processings and computations based on the quantum physics can go far beyond those based on classical physics. At its heart, this is because the potential ability of a probability is enlarged from classical theory to quantum theory. Indeed, quantum theory can be considered as a probabilistic theory, which — in some sense — properly includes the classical probability theory (Kolmogorov’s probability theory). However, this does not mean that quantum theory is the most general theory of a probability even among the possible theories which have an operational meanings. So far, the most general theory of a probability with a suitable operational meanings has been developed by several researchers (See for instance [1, 2, 3, 4, 5, 6, 7]). Following the recent trend, we call such theories the *general probabilistic theories* (or simply GPTs).

As the quantum information theory has been constructed based on the quantum theory, information theories can be constructed based on each probabilistic theory [7, 8, 9, 10, 11, 12, 13, 14]. There are several motivations for this line of researches: First, this is an attempt to find physical principles (axioms written by physical languages) for quantum theory [15, 16, 17]. Indeed, by considering the general framework which encompasses the quantum theory, we look for principles which determine the position of the quantum theory in this general framework. The development of the quantum information theory motivate us to find the principles based on information processings for the theory of quantum physics [10, 18, 19]. Second, the construction of the information theory based on the most general theory of probability enables us to understand logical connections among information processings by resorting to the particular properties of neither classical nor quantum theory, but only to

the essential properties which a suitable probability theory should possess. Third, this is a preparation for the possible break of quantum theory. For instance, one can discuss a secure key distribution in the general framework without assuming quantum theory itself [20]. Finally, this might provide a classical information theory under some restrictions of measurements, since any general probabilistic theories has a classical interpretation based on such restrictions of measurements [3, 21].

In this paper, we propose and give systematic discussions of several distinguishability measures (especially, *Kolmogorov distance* and *fidelity*) and three quantities related to entropies for general probabilistic theories. The corresponding measures and entropies in classical and quantum theory have been proved to be useful [24, 25], and we give generalizations for them in any GPTs and discuss their applications. In particular, no-cloning theorem and a simple information-disturbance theorem in GPTs are reformulated using fidelity, and a bound of the accessible information is discussed based on one of the “entropies”. Finally, we introduce and formulate the principle of “equality of pure states” meaning that there are no special pure states. We call such GPT symmetric and in symmetric GPT, the measure of pureness will be discussed.

## II. GENERAL PROBABILISTIC THEORIES

In this section, we give a brief review of general probabilistic theories (See for instance [1, 2, 3, 7] and references therein for details.) Although, in the end, we are going to use mathematical notions such as convexity, affine functions, etc., it should be noticed that we do not assume any mathematical structure without physical reasons.

The important ingredients of the GPTs are the notions of state and measurement. In any GPT, we have a physical law to determine a probability  $p(a|M, s)$  to obtain an output  $a$  by a measurement  $M$  of an observable under a state  $s$ . In this paper, for simplicity, we only treat a measurement with a finitely many outcomes. Naturally, we assume the separating properties of both states

\*Electronic address: gen-kimura[at]aist.go.jp

†Electronic address: k.nuida[at]aist.go.jp

and measurements: (A1) States  $s_1$  and  $s_2$  are identified if  $p(a|M, s_1) = p(a|M, s_2)$  for any measurement  $M$  and measurement outcome  $a$ ; (A2) Measurement  $M_1$  and  $M_2$  are identified if  $p(a|M_1, s) = p(a|M_2, s)$  for any measurement outcome  $a$  under any state  $s$ . We also assume the convex property of states; (A3) For any states  $s_1, s_2$  and  $q \in [0, 1]$ , there exists the state  $s$  to prepare  $s_1$  with probability  $q$  and  $s_2$  with probability  $1 - q$ ; namely, it follows that  $p(a|M, s) = qp(a|M, s_1) + (1 - q)p(a|M, s_2)$  for any measurement; (A4) Further, we naturally assume that the dynamics preserves this probabilistic mixtures; (A5) We introduce a natural topology on the state space which is the weakest topology such that  $s \rightarrow p(a|M, s)$  is continuous for any measurements; Finally, we assume (A6) a joint state  $\omega$  of system  $A + B$  defines a joint probability for each measurements  $M_A$  and  $M_B$  which satisfies the no-signaling condition, i.e., the marginal probabilities for the outcomes of a measurement on  $A$  do not depend on the measurement choices on  $B$ , and vice versa. Moreover, the joint state is determined by joint probabilities for all pairs of measurements of  $A$  and  $B$ .

Based on these, one can show the followings [1, 2, 3, 7]:

(a) There exists a locally convex topological vector space  $V$  such that, in a suitable representation, *the state space  $\mathcal{S}$  is a convex subset in  $V$  where  $qs_1 + (1 - q)s_2$  corresponds to the state described in (A3) above.* An extreme point of  $\mathcal{S}$  is called a pure state. Moreover, without loss of generality, one can assume that  $\mathcal{S}$  is compact with a natural topology [13]. Notice that by the famous Krein-Milman theorem (see, for instance, Theorem 10.4 in [22]) the set of extreme points  $\mathcal{S}_{\text{pure}}$  is non-empty and  $\mathcal{S}$  is the closed convex hull of extreme points. In particular, in finite dimensional cases, any state  $s \in \mathcal{S}$  has a convex decomposition with finite numbers of pure states (hereafter, *a pure state decomposition*):  $s = \sum_x p_x s_x$  where  $p_x \geq 0$ ,  $\sum_x p_x = 1$ ,  $s_x \in \mathcal{S}_{\text{pure}}$  (see, for instance, Theorem 5.6 in [23]).

A map  $f : \mathcal{S} \rightarrow \mathbb{R}$  is called an affine functional if it satisfies  $f(qs_1 + (1 - q)s_2) = qf(s_1) + (1 - q)f(s_2)$  for any  $q \in [0, 1]$ ,  $s_1, s_2 \in \mathcal{S}$ . In particular an affine functional  $e : \mathcal{S} \rightarrow \mathbb{R}$  is called an effect if the range is contained in  $[0, 1]$ . We denote the sets of all the affine functional and all the effects by  $\mathcal{A}(\mathcal{S})$  and  $\mathcal{E}(\mathcal{S})$ , respectively. It is easy to see that  $\mathcal{E}(\mathcal{S})$  is a convex subset of a real vector space  $\mathcal{A}(\mathcal{S})$ . We call an extreme effect a *pure effect*. The zero effect  $0$  and unit effect  $u$  such that  $0(s) = 0$  and  $u(s) = 1$  are trivially pure effects. It is easy to see that effect  $u - e$  is pure iff effect  $e$  is pure. Moreover, we can introduce a natural topology on  $\mathcal{E}(\mathcal{S})$  which is the weakest topology such that the map  $\mathcal{E}(\mathcal{S}) \rightarrow \mathbb{R}$ ,  $e \mapsto e(s)$ , becomes continuous for every  $s \in \mathcal{S}$ . One can that  $\mathcal{E}(\mathcal{S})$  is compact with respect to this topology [13].

(b) It is often convenient to characterize a measurement without explicitly specifying the measurement outcomes. In that case, *any measurement  $M$  is characterized by the set of effects  $m_i$  such that  $p(a_i|M, s) = m_i(s)$  and  $\sum_i m_i = u$ :* In the following, we occasionally use the notation  $M = (m_j)_j$  (implicitly assuming conditions

$m_j \in \mathcal{E}(\mathcal{S})$  and  $\sum_j m_j = u$ ) to denote the measurement on  $\mathcal{S}$  meaning that  $m_j(s)$  is the probability to obtain  $j$ th output (say  $a_j$ ) by a measurement  $M$  under a state  $s$ .

(c) *Dynamics is described by an affine function on state space.* In general, the initial state space  $\mathcal{S}$  and final state space  $\mathcal{S}'$  might be different. Then, a time evolution map is given by an affine map  $f$  from  $\mathcal{S}$  to  $\mathcal{S}'$ . We denote by  $\mathcal{A}(\mathcal{S}, \mathcal{S}')$  the set of all the affine map from  $\mathcal{S}$  to  $\mathcal{S}'$ .

(d) The joint systems are described by a convex set in a tensor product of the corresponding vector spaces. A joint state  $\omega$  on  $A + B$  with state spaces  $\mathcal{S}_A$  and  $\mathcal{S}_B$  is described by a bi-affine map on  $\mathcal{E}(\mathcal{S}_A) \times \mathcal{E}(\mathcal{S}_B)$ . In particular, if  $\omega$  is a joint state on  $A + B$ , then the marginal state of  $A$  is defined by  $\omega_A(e) := \omega(e, u_B)$  ( $e \in \mathcal{E}(\mathcal{S}_A)$ ) where  $u_B$  is the unit effect on  $\mathcal{S}_B$ . From the extreme property of pure states, it is easy to see [33] that if the marginal state  $\omega_A$  is pure, then a joint state  $\omega$  is a state with no correlations:  $\omega(e_A, e_B) = \omega_A(e_A)\omega_B(e_B)$  ( $e_A \in \mathcal{E}(\mathcal{S}_A), e_B \in \mathcal{E}(\mathcal{S}_B)$ ).

It is important to notice that all the mathematical structures are not introduced *ad hoc* but they appear naturally based on physical assumptions (A1-A6). It is also possible to formulate the measurement process by considering the cone generated by  $0$  and  $\mathcal{S}$  in  $V$  [2, 5, 10].

In this paper, we treat for simplicity finite GPT where  $V$  is finite dimensional, but most of the definitions and properties below holds with some topological remarks [22]. (However, notice that in finite dimensional cases, there are essentially the unique topology, and one can use another characterization of the natural topology, for instance using the Kolmogorov distance below. In particular, the unique topology is the Euclidean topology and thus one can imagine a state space of each GPT as any compact convex (or equivalently closed bounded convex) subset in Euclidean spaces.) Moreover, we assume that any set of effects  $m_i$  such that  $\sum_i m_i = u$  has a correspondent measurement. (It is also easy exercises to reformulate below without this assumption.)

Here, let us see the typical examples for finite GPTs.

[Finite Classical Systems] Let  $\Omega = \{\omega_1, \dots, \omega_d\}$  be a sample space. The state is represented by a probability  $p_i$  for an elementary event  $\omega_i$ . The state space is given by  $\mathcal{S}_c := \{\mathbf{p} \in \mathbb{R}^d \mid p_i \geq 0, \sum_{i=1}^d p_i = 1\}$ . There are  $d$  numbers of pure states, which are the definite states where one of the elementary event occurs with probability 1: Namely,  $\mathbf{p}^{(\mu)} = (\delta_{\mu 1}, \dots, \delta_{\mu d}) \in \mathcal{S}_c$  ( $\mu = 1, \dots, d$ ) Notice that  $\mathcal{S}_c$  is a (standard) simplex. In particular, any state  $\mathbf{p} = (p_1, \dots, p_d) \in \mathcal{S}_c$  has the unique pure state decomposition:  $\mathbf{p} = \sum_{\mu=1}^d p_\mu \mathbf{p}^{(\mu)}$ .

[Finite Quantum Systems] Let  $\mathcal{H}$  be a  $d$  dimensional complex Hilbert space. A quantum state is represented by a density operator  $\rho$ , i.e., a positive operator on  $\mathcal{H}$  with unit trace. The state space is given by  $\mathcal{S}_q = \{\rho \in \mathcal{L}(\mathcal{H}) \mid \rho \geq 0, \text{tr} \rho = 1\}$  where  $\mathcal{L}(\mathcal{H})$  is a real vector space of all the (Hermitian) operator on  $\mathcal{H}$ . Pure states are characterized by 1 dimensional projection operators. A quantum effect  $e$  is represented by an operator  $E$  satisfying  $0 \leq E \leq \mathbb{I}$ , called a POVM (positive op-

erator valued measure) element, by the correspondence  $e(\rho) = \text{tr}(\rho E)$ . Here  $0, \mathbb{I}$  denote the zero and identity operator on  $\mathcal{H}$ . In particular, any measurement of an observable  $M = (m_i)_i$  where  $m_i$  are effects on  $\mathcal{S}_q$  has the correspondent POVM measurement  $(M_i)_i$  such that  $M_i \in \mathcal{L}(\mathcal{H})$ ,  $M_i \geq 0$ ,  $\sum_i M_i = \mathbb{I}$  and  $m_i(\rho) = \text{tr}(\rho M_i)$ . Notice that the set of all the extreme effects is the set of all the projection operator  $\mathcal{P}(\mathcal{H})$ . The POVM measurement  $(P_i)_i$  consists of projection operators  $P_i$  is called a PVM (projection valued measure) measurement. The following is an example of GPT which is neither classical nor quantum:

[Hyper Cuboid Systems and squared system] Let  $\mathcal{S}_{cb} := \{c \in \mathbb{R}^d | 0 \leq c_i \leq 1 (i = 1, \dots, d)\}$ . The pure states are  $2^d$  numbers of vertexes. We call this *hyper cuboid system* and especially the *squared system* when  $d = 2$  [11]. These might be the easiest examples of GPT which are neither classical nor quantum. However, one can construct a classical model such that a suitable restriction of measurements reduces the hyper cuboid systems [21].

Finally, notice that the probabilistic theories with state spaces  $\mathcal{S}_A$  and  $\mathcal{S}_B$  are equivalent if they are affine isomorphic, i.e., there exists a bijective affine map from  $\mathcal{S}_A$  to  $\mathcal{S}_B$ . For instance, any GPT which has a simplex state space is affine isomorphic to some standard simplex, and therefore can be considered as a classical system.

### III. DISTINGUISHABILITY MEASURES FOR GENERAL PROBABILISTIC THEORIES

In this section, we introduce several distinguishability measures (Kolmogorov distance, Fidelity, Shannon distinguishability etc) for GPTs. The corresponding measures for quantum systems are proved to be useful in quantum information theories [24]. It is indeed straightforward to generalize them to any GPT using the notions developed in the preceding sections, and some of them has been used in references [10, 12, 13]. Most of the properties for quantum systems preserves to be hold including the ways to prove them [24]. However, we think it useful to sum up these measures, especially Kolmogorov distance and fidelity, for GPT systematically and all the proofs of this section are put in Appendix A for the reader's convenience. A striking thing is that all the below results does not resort to ingredients such as vectors and operators on a Hilbert space, but only to the analysis of probabilities.

All the measures below are based on those for classical systems among every possible measurements of observables: In the following, let  $\mathcal{S}$  be the set of states (state space), and  $\mathcal{E} = \mathcal{E}(\mathcal{S})$ ,  $\mathcal{M} = \mathcal{M}(\mathcal{S})$  be the sets of effects and measurements on  $\mathcal{S}$ .

#### A. Kolmogorov Distance in GPT

The Kolmogorov distance  $D_c(\mathbf{p}, \mathbf{q})$  is known to serve as a good distinguishability measure between two probability distributions  $\mathbf{p} = (p_i)_i$  and  $\mathbf{q} = (q_j)_j$ :

$$D_c(\mathbf{p}, \mathbf{q}) := \frac{1}{2} \sum_i |p_i - q_i|.$$

Indeed,  $D_c$  has a metric property and it follows that  $D_c(p_i, q_j) = \max_S |p(S) - q(S)|$  where the maximization is taken over all subsets  $S$  of the index set  $\{i\}$ . Thus  $D_c(\mathbf{p}, \mathbf{q})$  is considered as a metric for two probability distributions with an operational meaning.

In any GPT, one can define [13] the Kolmogorov distance between two states  $s_1, s_2 \in \mathcal{S}$  by

$$D(s_1, s_2) := \max_{M=(m_i) \in \mathcal{M}} D_c(\mathbf{p}_1(M), \mathbf{p}_2(M)), \quad (1)$$

where  $\mathbf{p}_1(M) := (m_i(s_1))_i$  and  $\mathbf{p}_2(M) := (m_i(s_2))_i$  are probability distributions to get  $i$ th output of the measurement  $M$  under states  $s_1$  and  $s_2$ , respectively. The maximization in (1) is always attained by some measurement, which we call an optimal measurement, due to the compactness of the effect set [13]. Notice that  $D(s_1, s_2)$  is a metric of  $\mathcal{S}$ , i.e., (i)  $D(s_1, s_2) \geq 0$ ; equality iff  $s_1 = s_2$ , (ii)  $D(s_1, s_2) = D(s_2, s_1)$ , and (iii)  $D(s_1, s_3) \leq D(s_1, s_2) + D(s_2, s_3)$ , and it is bounded above from 1, i.e.,  $0 \leq D(s_1, s_2) \leq 1$ . These follow from a metric property of  $D_c$  and a separation property of states. The above mentioned operational meaning of  $D_c$  also gives  $D(\rho, \sigma)$  an operational meaning; that is the maximum difference of probability among all the event  $S$  and all measurements. In quantum systems,  $D(\rho_1, \rho_2)$  is the trace distance between density operators  $\rho_1, \rho_2$ :  $D(\rho_1, \rho_2) = \frac{1}{2} \text{tr} |\rho_1 - \rho_2|$  [25] where  $|A| := \sqrt{A^\dagger A}$ .

For any measurement  $M = (m_i)$  and states  $s_1, s_2 \in \mathcal{S}$ , one can consider a two valued measurement  $M_2 = (m_+, m_-)$  where  $m_+ := \sum_{i \in X_+} m_i$  and  $m_- := \sum_{i \in X_-} m_i$  with  $X_+ := \{i \mid m_i(s_1) - m_i(s_2) \geq 0\}$  and  $X_- := \{i \mid m_i(s_1) - m_i(s_2) < 0\}$ . Using this, one has another characterization of the Kolmogorov distance:

$$D(\rho, \sigma) = \max_{e \in \mathcal{E}} (e(\rho) - e(\sigma)). \quad (2)$$

The quantity in the right-hand side is a metric used in [10].

Let  $P_s(s_1, s_2)$  be the maximal success probability to distinguish two states  $s_1$  and  $s_2$  in a single measurement under the uniform prior distribution. Without loss of generality, it is enough to consider two-valued measurement  $(m_1, m_2) \in \mathcal{M}$  for a discrimination problem of two states  $s_1$  and  $s_2$  by guessing  $s_1$  (or  $s_2$ ) when observing 1 (or 2)th output. Thus, we have

$$\begin{aligned} P_s(s_1, s_2) &:= \max_{(m_1, m_2) \in \mathcal{M}} \left( \frac{1}{2} m_1(s_1) + \frac{1}{2} m_2(s_2) \right) \\ &= \frac{1}{2} \left( 1 + \max_{e \in \mathcal{E}} (e(s_1) - e(s_2)) \right). \end{aligned} \quad (3)$$

From (2) and (3), we have another operational meaning of the Kolmogorov distance:

**Proposition 1** *For any states  $s_1, s_2 \in \mathcal{S}$  in GPT,*

$$D(s_1, s_2) = 2P_s(s_1, s_2) - 1.$$

Note that  $D(s_1, s_2)$  takes the maximum 1 iff  $P_s(s_1, s_2) = 1$ , i.e., when  $s_1$  and  $s_2$  are completely distinguishable in a single measurement. On the other hand,  $D(s_1, s_2)$  takes the minimum 0 (thus  $s_1 = s_2$ ) iff  $P_s(s_1, s_2) = 1/2$ , i.e.,  $s_1$  and  $s_2$  are completely indistinguishable (and indeed such states should be identified due to the separation property of states).

In the following, we show the monotonicity, strong convexity, joint convexity, and convexity follow for the Kolmogorov distance in any GPT.

**Proposition 2 (Monotonicity)** *For any states  $s_1, s_2 \in \mathcal{S}$ , and time evolution map  $\Lambda \in \mathcal{A}(\mathcal{S}, \mathcal{S}')$ , we have*

$$D(s_1, s_2) \geq D(\Lambda(s_1), \Lambda(s_2)).$$

This implies that the distinguishability between  $s_1$  and  $s_2$  cannot be increased in any physical means. Notice that it is well known that the trace distance in quantum systems has the monotonicity property under any trace preserving completely positive map [25]. Proposition 2 generalizes this for any trace preserving positive map.

**Proposition 3 (Strong convexity)** *Let  $\mathbf{p} = (p_i)_i$  and  $\mathbf{q} = (q_i)_i$  be probability distributions over the same index set, and  $s_i, t_i \in \mathcal{S}$  be states of GPT with the same index set. Then, it follows that*

$$D\left(\sum_i p_i s_i, \sum_i q_i t_i\right) \leq D_c(\mathbf{p}, \mathbf{q}) + \sum_i p_i D(s_i, t_i).$$

As corollaries, we have

**Corollary 1 (Joint convexity)**

$$D\left(\sum_i p_i s_i, \sum_i p_i t_i\right) \leq \sum_i p_i D(s_i, t_i).$$

(As a special case  $p_i = q_i$  of the strong convexity.)

**Corollary 2 (Convexity)**

$$D\left(\sum_i p_i s_i, t\right) \leq \sum_i p_i D(s_i, t).$$

(As a special case  $t_i = t$  of the joint convexity.)

## B. Fidelity in GPT

The Bhattacharyya coefficient (the classical fidelity) between two probability distributions  $\mathbf{p} = (p_i)_i$  and  $\mathbf{q} = (q_j)_j$  is defined by :

$$F_c(\mathbf{p}, \mathbf{q}) := \sum_i \sqrt{p_i q_i}. \quad (4)$$

Note that (i)  $0 \leq F_c(\mathbf{p}, \mathbf{q}) \leq 1$  where  $F_c(\mathbf{p}, \mathbf{q}) = 1$  iff  $\mathbf{p} = \mathbf{q}$ ; (ii)  $F_c(\mathbf{p}, \mathbf{q}) = F_c(\mathbf{q}, \mathbf{p})$ . We say two probability distributions  $\mathbf{p}, \mathbf{q}$  are orthogonal iff  $F_c(\mathbf{p}, \mathbf{q}) = 0$ .

In any GPT, one can also define the fidelity [2, 12] between two states  $s_1, s_2 \in \mathcal{S}$  as

$$F(s_1, s_2) = \inf_{M=\{m_i\} \in \mathcal{M}} F_c(\mathbf{p}_1(M), \mathbf{p}_2(M)), \quad (5)$$

where  $\mathbf{p}_1(M) := (m_i(s_1))_i$  and  $\mathbf{p}_2(M) := (m_i(s_2))_i$ . Contrast to the Kolmogorov distance, the attainability of the infimum of the fidelity seems to be nontrivial. In quantum mechanics, one has the formula  $F(\rho_1, \rho_2) = \text{tr}[\rho_1^{1/2} \rho_2^{1/2}] = \text{tr}[(\rho_1^{1/2} \rho_2 \rho_1^{1/2})^{1/2}]$  between two density operators  $\rho_1, \rho_2$  [25, 26]. Also, it is shown that an optimal measurement (POVM) exists which attains the infimum.

From the property of the Bhattacharyya coefficient and the separation property of states, it follows that (i)  $0 \leq F(s_1, s_2) \leq 1$  where  $F(s_1, s_2) = 1$  iff  $s_1 = s_2$ ; (ii)  $F(s_1, s_2) = F(s_2, s_1)$ . We say that states  $s_1$  and  $s_2$  are orthogonal ( $s_1 \perp s_2$ ) iff  $F(s_1, s_2) = 0$ .

**Proposition 4 (Monotonicity)** *For any states  $s_1, s_2 \in \mathcal{S}$ , and time evolution map  $\Lambda \in \mathcal{A}(\mathcal{S}, \mathcal{S}')$ , it follows*

$$F(\Lambda(s_1), \Lambda(s_2)) \geq F(s_1, s_2).$$

**Proposition 5 (Strong concavity [12])** *Let  $\mathbf{p} = (p_i)_i$  and  $\mathbf{q} = (q_i)_i$  be probability distributions over the same index set, and  $s_i, t_i \in \mathcal{S}$  be states of GPT with the same index set. Then,*

$$F\left(\sum_i p_i s_i, \sum_i q_i t_i\right) \geq \sum_i \sqrt{p_i q_i} F(s_i, t_i).$$

As corollaries, one gets

**Corollary 3 (Joint concavity and concavity)**

$$\begin{aligned} F\left(\sum_i p_i s_i, \sum_i p_i t_i\right) &\geq \sum_i p_i F(s_i, t_i), \\ F\left(\sum_i p_i s_i, t\right) &\geq \sum_i p_i F(s_i, t). \end{aligned}$$

**Proposition 6** *In a bipartite system  $A+B$ , we have the followings:*

(i)  $F(s_A, t_A) \geq F(s, t)$  for any  $s, t \in \mathcal{S}_A \otimes \mathcal{S}_B$  where  $s_A$  and  $t_A$  are the reduced states to the system  $A$ .

(ii)  $F(s_1, s_2) F(t_1, t_2) \geq F(s_1 \otimes t_1, s_2 \otimes t_2)$  for any  $s_1, s_2 \in \mathcal{S}_A, t_1, t_2 \in \mathcal{S}_B$ .

(iii)  $F(s_1, s_2) = F(s_1 \otimes t, s_2 \otimes t)$  for any  $s_1, s_2 \in \mathcal{S}_A, t \in \mathcal{S}_B$ .

In particular, from (ii), it follows

$$F(s, t)^2 \geq F(s \otimes s, t \otimes t), \quad (6)$$

by letting  $\mathcal{S} := \mathcal{S}_A = \mathcal{S}_B$  and  $s = s_1 = t_1 \in \mathcal{S}$  and  $t = s_2 = t_2 \in \mathcal{S}$ .

Note that the generalization of properties of Proposition 6 is straightforward for multipartite system.



However, contrary to the Kolmogorov distance, it is difficult to give an operational meaning for the Fidelity, since there is no known operational meaning of Bhattacharyya coefficient. In using the Fidelity, it is important to know the relation with another operational measures like the Kolmogorov distance.

### C. Relation between the Kolmogorov Distance and the Fidelity

**Proposition 7** *For any state  $s, t \in \mathcal{S}$ , it follows*

$$1 - F(s, t) \leq D(s, t) \leq \sqrt{1 - F(s, t)^2}. \quad (7)$$

This relation is famous to hold in quantum systems [24, 25], but Proposition 7 shows that this holds for any GPT.

From (7), we have

**Corollary 4** *(i)  $D(s, t) = 0$  iff  $F(s, t) = 1$  and (ii)  $D(s, t) = 1$  iff  $F(s, t) = 0$ . In particular, the orthogonality of states turns out to be equivalent to the complete distinguishability of states ( $P_s = 1$ ).*

In this sense, the Kolmogorov distance and the fidelity is equivalent.

Similarly, it is straightforward to introduce another measures which are used in quantum information theory. For instance, one can define Shannon distinguishability and can show the same relations (see for instance Theorem 1 in [24]).

## IV. APPLICATIONS

In this section, we give simple proofs using the Fidelity for no-cloning theorem [7] and information-disturbance theorem [12, 13] in any GPT.

**Theorem 1 (No-cloning)** *In any GPT, two states  $s_1, s_2 \in \mathcal{S}$  are jointly clonable iff  $s_1 = s_2$  or  $s_1$  and  $s_2$  are completely distinguishable.*

**Proof** Let states  $s_1, s_2 \in \mathcal{S}$  are jointly clonable. Namely, there exists a time evolution map (a cloning machine)  $\Lambda \in \mathcal{A}(\mathcal{S}, \mathcal{S} \otimes \mathcal{S})$  satisfying

$$\Lambda(s_1) = s_1 \otimes s_1, \quad \Lambda(s_2) = s_2 \otimes s_2. \quad (8)$$

From (6), we have

$$F(\Lambda(s_1), \Lambda(s_2)) = F(s_1 \otimes s_1, s_2 \otimes s_2) \leq F(s_1, s_2)^2.$$

From the monotonicity of  $F$ , it follows that  $F(s_1, s_2) \leq F(\Lambda(s_1), \Lambda(s_2)) \leq F(s_1, s_2)^2$ , which implies that  $F(s_1, s_2) = 0$  or 1. In other words,  $s_1 = s_2$  or  $s_1$  and  $s_2$  are completely distinguishable (cf. Corollary 4).

Suppose that  $s_1 = s_2$ , then one has a time evolution map  $\Lambda \in \mathcal{A}(\mathcal{S}, \mathcal{S} \otimes \mathcal{S})$  defined by  $\Lambda(s) := s \otimes s$ . (Physically, this is nothing but a preparation of a fixed

state  $s_1$ .) It is obvious that this jointly clones  $s_1$  and  $s_2$ . Next, suppose that  $s_1$  and  $s_2$  are completely distinguishable. Namely, there exists a measurement  $M = (m_1, m_2) \in \mathcal{M}(\mathcal{S})$  such that  $m_1(s_1) = 1, m_1(s_2) = 0$  (and thus  $m_2(s_1) = 0, m_2(s_2) = 1$ ). Then,  $\Lambda(s) := m_1(s)s_1 \otimes s_1 + m_2(s)s_2 \otimes s_2$  for any  $s \in \mathcal{S}$  defines a time evolution map  $\Lambda \in \mathcal{A}(\mathcal{S}, \mathcal{S} \otimes \mathcal{S})$  satisfying the cloning condition (8). (Notice that  $m_1(s), m_2(s) \geq 0, m_1(s) + m_2(s) = 1$  and thus  $m_1(s)s_1 \otimes s_1 + m_2(s)s_2 \otimes s_2 \in \mathcal{S} \otimes \mathcal{S}$  from the convexity of  $\mathcal{S} \otimes \mathcal{S}$ . The affinity of  $\Lambda$  follows from the affinity of  $m$ .) ■

**Lemma 1** *For any GPT with at least two distinct states, there exists two distinct states which are not completely distinguishable.*

**Proof** Let  $s_1 \neq s_2 \in \mathcal{S}$ . Assume that any two distinct states are completely distinguishable. Then, we have  $F(s_1, s_2) = 0$ . From the convexity of  $\mathcal{S}$ , there exists a state  $s := \frac{1}{2}s_1 + \frac{1}{2}s_2 \neq s_1$ . From the concavity of  $F$ , we have  $F(s_1, s) \geq \frac{1}{2}F(s_1, s_1) + \frac{1}{2}F(s_1, s_2) = \frac{1}{2}$ . Therefore,  $s_1$  and  $s$  are distinct states which are not completely distinguishable. ■

We call a physical process which clones any unknown states a *universal cloning machine* :

**Proposition 8 (No-cloning)** *In any GPT with at least two distinct states, there are no universal cloning machine.*

**Proof** This follows from Theorem 1 and Lemma 1. ■

In a usual application, cloning is often considered for only pure states. We call a physical process which clones any unknown pure states a *universal cloning machine for pure states* : However, such cloning is possible if and only if GPT is classical:

**Proposition 9** *GPT is classical iff there is a universal cloning machine for pure states.*

**Proof** Notice that classical systems are characterized by the fact that all the pure states are completely distinguishable [7]. This fact and Theorem 1 complete the proof. ■

**Theorem 2 (Information disturbance)** *In any GPT, any attempt to get information to discriminate two pure states which are not completely distinguishable inevitably causes disturbance.*

**Proof** Let  $s_1, s_2 \in \mathcal{S}_A$  be two pure states which are not completely distinguishable, i.e.,  $0 < F(s_1, s_2)$ . Assume that there is a physical mean to get information to discriminate  $s_1, s_2$  without causing any disturbance to the system. This implies that we have a time evolution map  $\Lambda \in \mathcal{A}(\mathcal{S}_A, \mathcal{S}_A \otimes \mathcal{S}_B)$  and initial states  $t_0 \in \mathcal{S}_B$  such that the reduced states to system A is the same:

$$\Lambda(s_1 \otimes t_0)_A = s_1, \quad \Lambda(s_2 \otimes t_0)_A = s_2.$$

Since  $s_1, s_2$  are pure states, there exists no correlations between system A and B, and hence one gets

$$\Lambda(s_1 \otimes t_0) = s_1 \otimes t_1, \quad \Lambda(s_2 \otimes t_0) = s_2 \otimes t_2,$$

for some  $t_1, t_2 \in \mathcal{S}_B$ . From the monotonicity of  $F$  and Proposition 6, it follows that  $F(s_1, s_2) = F(s_1 \otimes t_0, s_2 \otimes t_0) \leq F(\Lambda(s_1 \otimes t_0), \Lambda(s_2 \otimes t_0)) = F(s_1, s_2)F(t_1, t_2)$ . Since  $0 < F(s_1, s_2)$ , we have  $F(t_1, t_2) = 1$  and thus  $t_1 = t_2$ . Therefore, to get information to distinguish  $s_1$  and  $s_2$ , one has to inevitably disturb at least one of these states. ■

No cloning theorems are discussed in [7] with completely different methods. In [13], we have proved Theorem 2 using the Kolmogorov distance. Essentially the same proof as above is given in [12].

## V. INDECOMPOSABLE AND COMPLETE MEASUREMENT IN GENERAL PROBABILISTIC THEORIES

### A. Indecomposable Effect

In quantum systems, a fundamental POVM element  $E$  is that with one dimensional range, called a rank-one POVM element. Let us define the corresponding notions in any GPT, which we are going to call an *indecomposable* effect:

**Definition 1** We call an effect  $e \in \mathcal{E}(\mathcal{S})$  *indecomposable* if (i)  $e \neq 0$  and (ii) for any decomposition  $e = e_1 + e_2$  into the sum of two effects  $e_1$  and  $e_2$ , there exists  $c \in \mathbb{R}$  such that  $e_1 = ce$ . We denote the set of all the indecomposable effects on  $\mathcal{S}$  by  $\mathcal{E}_{\text{ind}}(\mathcal{S}) \subset \mathcal{E}(\mathcal{S})$ .

It is easy to see that the above mentioned  $c$  satisfies  $0 \leq c \leq 1$ .

Here, we show some general properties of effects and indecomposable effects:

**Proposition 10** Let  $e$  be a non-zero pure effect on  $\mathcal{S}$ . Then, there exists a state  $s$  such that  $e(s) = 1$ . Since  $\mathcal{S}$  is compact, such state can be taken to be a pure state.

**Proof** Suppose that there are no state  $s$  such that  $e(s) = 1$ . Then, from the compactness of  $\mathcal{S}$ , we have

$$\sup_{s \in \mathcal{S}} e(s) = \max_{s \in \mathcal{S}} e(s) =: x < 1.$$

From this,  $\tilde{e} := e/x$  is an effect which is neither  $e$  nor zero effect 0. Since we have the identity,

$$e = x\tilde{e} + (1-x)0,$$

this contradicts that  $e$  is a pure effect.

Let  $s = \sum_i p_i s_i$  ( $p_i > 0, \sum_i p_i = 1$ ) be a pure state decomposition of  $s$ . Then, it is easy to see  $e(s_i) = 1$  for any pure state  $s_i$ . Thus, we can take a pure state  $s$  such that  $e(s) = 1$ . ■

**Corollary 5** Let  $e$  be a pure effect which is not  $u$ . Then, there exists a state  $s$  such that  $e(s) = 0$ . Such state can be taken to be a pure state.

**Proof** Since  $e(\neq u)$  is pure, the effect  $\tilde{e} = u - e$  is non-zero pure effect. From Proposition 10, there exists a pure state  $s$  such that  $\tilde{e}(s) = 1 - e(s) = 1$ . Thus,  $e(s) = 0$ . ■

Next, we show that any non-zero effect has a decomposition with respect to indecomposable effects:

**Proposition 11** In any GPT, for every  $0 \neq e \in \mathcal{E}(\mathcal{S})$ , there exist a finite collection of indecomposable effects  $e_i \in \mathcal{E}(\mathcal{S}), 1 \leq i \leq r$ , such that  $e = \sum_{i=1}^r e_i$ . In particular, in any GPT, there exists an indecomposable effect.

(See Appendix A for the proof.) Moreover, we have:

**Proposition 12** In any GPT, there exists an indecomposable and pure effect.

**Proof** To prove this, we use the following lemmas:

**Lemma 2** Let  $e \in \mathcal{E}$  be an indecomposable effect and let  $q := \max_{s \in \mathcal{S}} e(s)$ . (Note that  $0 < q \leq 1$ .) Then,  $\tilde{e} := \frac{1}{q}$  is an indecomposable effect.

**Lemma 3** If  $e$  is indecomposable effect such that there exists a state  $s$  satisfying  $e(s) = 1$ , then  $e$  is a pure effect.

(See appendix A for the proofs.) From Proposition 11, there exists an indecomposable effect. From Lemma 2, one can construct an indecomposable effect from any indecomposable effect such that  $\tilde{e}(s) = 1$  for some pure state. From Lemma 3, it is an indecomposable and pure effect. ■

In the following, we give a characterization of indecomposable effects in classical, quantum and hyper cuboid systems in order:

[Classical Systems] Let  $\mathcal{S}_c$  be the state space of a classical system introduced in section II. Remind that any state  $\mathbf{p} = (p_1, \dots, p_d) \in \mathcal{S}_c$  has the unique decomposition with respect to pure states:  $s = \sum_{\mu} p_{\mu} \mathbf{p}^{(\mu)}$ . Thus, an effect  $e$  on  $\mathcal{S}_c$  is completely characterized by  $d$  numbers of value  $x_{\mu} := e(\mathbf{p}^{(\mu)}) \in [0, 1]$  ( $\mu = 1, \dots, d$ ). Conversely, for any given  $x_{\mu} \in [0, 1]$  ( $\mu = 1, \dots, d$ ), there exists an effect  $e$  such that  $e(\mathbf{p}^{(\mu)}) = x_{\mu}$ . Let  $e^{(\mu)} \in \mathcal{E}(\mathcal{S}_c)$  ( $\mu = 1, \dots, d$ ) be the effects defined by  $e^{(\mu)}(\mathbf{p}^{(\nu)}) = \delta_{\mu\nu}$ . In classical systems, the indecomposable effect is characterized as follows:

**Proposition 13** An effect  $e \in \mathcal{E}(\mathcal{S}_c)$  is indecomposable iff there is one pure state at which the value of effect is non-zero. In other words,  $\mathcal{E}_{\text{ind}}(\mathcal{S}_c)$  is characterized by  $\mathcal{E}_{\text{ind}}(\mathcal{S}_c) = \{\lambda e^{(\mu)} \mid \lambda \in (0, 1], \mu = 1, \dots, d\}$ .

**[Proof]** First, let  $e$  be an effect such that there exists one pure state, say  $\mathbf{p}^{\mu}$ , at which the value of effect is non-zero. Then, one has  $e \neq 0$  and  $e = \lambda e^{(\mu)} \in \mathcal{E}(\mathcal{S}_c)$  for some  $\lambda \in (0, 1]$ . Let  $e = f + g$  for  $f, g \in \mathcal{E}(\mathcal{S}_c)$ . Then  $f(\mathbf{p}^{(\nu)}) = 0$  for any  $\nu \neq \mu$ , and it follows that

$f = \frac{f(\mathbf{p}^{(\mu)})}{\lambda}e$ . Therefore,  $e$  is indecomposable. Next, let  $e$  be indecomposable effect. Assume that there are at least two non-zero pure states, say  $\mathbf{p}^{(\mu_0)}, \mathbf{p}^{(\mu_1)}$  ( $\mu_0 \neq \mu_1 = 1, \dots, d$ ) at which the effect values are non-zero. Let  $x_\mu := e(\mathbf{p}^{(\mu)})$ . Let  $f, g$  be effects defined by  $f(\mathbf{p}^{(\mu)}) = x_{\mu_0}\delta_{\mu\mu_0}$  and  $g = e - f$ . Obviously  $e \neq cf$  for any  $c \in \mathbb{R}$ , and it contradicts that  $e$  is indecomposable. Since  $e \neq 0$ , there is the only one pure state at which the value of effect is non-zero. ■

[Quantum Systems] Next, we show that indecomposable effects for quantum systems are characterized by an one dimensional projections, i.e., rank-one POVM element. Let  $\mathcal{H}$  be the  $d$  dimensional Hilbert space and let  $\mathcal{S}_q$  be the set of all the density operators on  $\mathcal{H}$ . We call a non-zero POVM element  $E$  indecomposable iff the corresponding effect  $e(\cdot) := \text{tr}(E\cdot)$  is indecomposable. It is easy to see that a POVM element  $E$  is one dimensional iff there exists  $\lambda \in (0, 1]$  and a unit vector  $\psi \in \mathcal{H}$  such that  $E = \lambda|\psi\rangle\langle\psi|$ .

**Proposition 14** *A POVM element  $E \in \mathcal{E}_q$  is indecomposable if and only if it is a rank-one POVM element.*

**Proof** Let  $E = \lambda|\psi\rangle\langle\psi|$  be a rank-one POVM element with a unit vector  $\psi \in \mathcal{H}$  and  $\lambda \in (0, 1]$ . Let  $E = E_1 + E_2$  for some POVM elements  $E_1, E_2$ :

$$\lambda|\psi\rangle\langle\psi| = E_1 + E_2. \quad (9)$$

Let  $\{\psi_n\}_n$  be an orthonormal basis of  $\mathcal{H}$  such that  $\psi_1 = \psi$ . Then, from (9), it follows that  $\langle\psi_j|E_1\psi_j\rangle = \|E_1^{1/2}\psi_j\|^2 = 0$  ( $\forall j \geq 2$ ), and hence  $E_1\psi_j = 0$  ( $\forall j \geq 2$ ). For any  $\xi \in \mathcal{H}$ , we have  $E_1\xi = E_1(\sum_n \langle\psi_n|\xi\rangle\psi_n) = \langle\psi|\xi\rangle E_1\psi = |E_1\psi\rangle\langle\psi|\xi$ . Thus,  $E_1$  has the form of  $|\phi\rangle\langle\psi|$  (where  $\phi := E_1\psi$ ). Finally, since  $E_1$  is Hermitian, it follows that there exists  $c' \in \mathbb{R}$  such that  $\phi = c'\psi$  and hence  $E_1 = c'|\psi\rangle\langle\psi| = cE$  where  $c := \frac{c'}{\lambda}$ . This implies that  $E$  is indecomposable. Next, let  $E$  be indecomposable. Assume that  $E$  is rank  $l$  POVM element for some  $l \geq 2$ , and let  $E = \sum_{n=1}^l c_n|\psi_n\rangle\langle\psi_n|$  ( $c_n \in (0, 1]$ ) be an eigenvalue decomposition of  $E$ . Let  $E_1 := c_1|\psi_1\rangle\langle\psi_1|$  and  $E_2 := \sum_{n=2}^l c_n|\psi_n\rangle\langle\psi_n|$ . Obviously, they are POVM elements satisfying  $E = E_1 + E_2$ . However, for any  $c \in \mathbb{R}$ , we have  $E \neq cE_1$  (For instance,  $E\psi_2 = c_2 \neq 0$  while  $cE_1\psi_2 = 0$ ). This contradicts that  $E$  is indecomposable. Since  $E \neq 0$ , we conclude that  $E$  is rank one POVM element. ■

[Hyper cuboid systems] Finally, let  $\mathcal{S}_{\text{cb}}$  be the state space of a  $d$  dimensional hyper cuboid system introduced in section II. To determine the indecomposable effects in  $\mathcal{S}_{\text{cb}}$ , we present a general lemma which is also useful in later arguments (see Appendix A for the proof):

**Lemma 4** *If the state space  $\mathcal{S}$  of a GPT contains at least two states, then for every indecomposable effect  $e \in \mathcal{E}(\mathcal{S})$  we have  $e(s) = 0$  for some  $s \in \mathcal{S}$ .*

By virtue of this lemma, we obtain the following characterization of indecomposable effects in  $\mathcal{S}_{\text{cb}}$ :

**Proposition 15** *An effect  $e \in \mathcal{E}(\mathcal{S}_{\text{cb}})$  is indecomposable if and only if it is nonzero and it takes 0 at a  $d - 1$  dimensional face (facet) of  $\mathcal{S}_{\text{cb}}$ .*

**Proof** First we consider the ‘if’ part. Suppose that  $e$  is nonzero and  $e$  takes 0 at a facet  $F$  of  $\mathcal{S}_{\text{cb}}$ . Fix a state  $s \in \mathcal{S}_{\text{cb}}$  such that  $s \notin F$ . Note that  $e(s) > 0$  since  $e$  is nonzero. If  $e$  decomposes as  $e = e_1 + e_2$  with  $e_1, e_2 \in \mathcal{E}(\mathcal{S}_{\text{cb}})$ , then  $e_1$  (hence  $e_2$ ) also takes 0 at  $F$ . This implies that  $e_1 = \lambda e$  where  $\lambda = e_1(s)/e(s) \in \mathbb{R}$ , hence  $e$  is indecomposable.

Second, we consider the ‘only if’ part. By Lemma 4, an indecomposable effect  $e$  takes 0 at some state, hence at some pure state in  $\mathcal{S}_{\text{cb}}$ . By symmetry, we may assume without loss of generality that  $e(s_0) = 0$  where  $s_0 = (0, 0, \dots, 0) \in \mathcal{S}_{\text{cb}}$ . Let  $s_i$  ( $i \in \{1, 2, \dots, d\}$ ) be the vertex of  $\mathcal{S}_{\text{cb}}$  such that its  $j$ -th component is  $\delta_{ij}$ . Then we have  $e = \sum_{i=1}^d e(s_i)e_i$  where  $e_i \in \mathcal{E}(\mathcal{S}_{\text{cb}})$  maps  $(c_1, c_2, \dots, c_d)$  to  $c_i$ . Since  $e$  is indecomposable, it follows that  $e = \lambda e_i$  for some  $1 \leq i \leq d$  and  $\lambda \in \mathbb{R}$ , therefore  $e$  takes 0 at the facet  $\{(c_1, \dots, c_d) \in \mathcal{S}_{\text{cb}} \mid c_i = 0\}$  of  $\mathcal{S}_{\text{cb}}$ . ■

For example, the indecomposable effects in the squared system (i.e., when  $d = 2$ ) are listed in Table I, where  $\alpha_1, \dots, \alpha_4 \in (0, 1]$  are parameters.

TABLE I: Indecomposable effects in  $\mathcal{S}_{\text{cb}}$ ,  $d = 2$

effect	value at			
	$(0, 0)$	$(0, 1)$	$(1, 0)$	$(1, 1)$
$e_1$	0	0	$\alpha_1$	$\alpha_1$
$e_2$	$\alpha_2$	$\alpha_2$	0	0
$e_3$	0	$\alpha_3$	0	$\alpha_3$
$e_4$	$\alpha_4$	0	$\alpha_4$	0

## B. Indecomposable and complete measurements

Using the indecomposable effects defined above, we define an indecomposable measurement in any GPT as follows:

**Definition 2** *In a GPT with a state space  $\mathcal{S}$ , we say that a measurement  $M = (m_j)_j$  is indecomposable if all  $m_j \in \mathcal{E}(\mathcal{S})$  are indecomposable. The set of all the indecomposable measurements is denoted by  $\mathcal{M}_{\text{ind}}(\mathcal{S})$  or simply by  $\mathcal{M}_{\text{ind}}$ .*

From Proposition 14, an indecomposable measurement is a generalization of a one-rank POVM measurement in quantum systems.

**Proposition 16** *In any GPT, there exists an indecomposable measurement, i.e.,  $\mathcal{M}_{\text{ind}}(\mathcal{S}) \neq \emptyset$ .*

**Proof** From Lemma 11, a decomposition of the unit effect  $u$  with respect to the indecomposable effects gives an indecomposable measurement. ■

In quantum systems, rank-one PVM measurement plays a fundamental role in the foundation of quantum physics, which describes a measurement of a non degenerate Hermitian operator. One can also define the correspondent notion in any GPT, which we call a *complete* measurement, as follows:

**Definition 3** *In a GPT with a state space  $\mathcal{S}$ , we say that a measurement  $M = (m_j)_j$  is complete if all  $m_j \in \mathcal{E}(\mathcal{S})$  are indecomposable and extreme. The set of all the complete measurements are denoted by  $\mathcal{M}_{\text{comp}}(\mathcal{S})$ , or simply by  $\mathcal{M}_{\text{comp}}$ .*

It is easy to see that the set of extreme effects for classical systems are characterized by  $\mathcal{E}(\mathcal{S}_c)_{\text{ex}} = \{e \in \mathcal{E}(\mathcal{S}_c) \mid e(\mathbf{p}^{(i)}) = 1 \text{ or } 0 \ (i = 1, \dots, d)\}$  [34]. Hence, from proposition 13, there is essentially the unique complete measurement in classical systems given by  $M_{\text{comp}} := (e^{(j)})_j$ , where  $e^j(\mathbf{p}^{(k)}) := \delta_{jk}$  ( $j, k = 1, \dots, d$ ). More precisely,  $M = (m_j)_j$  is a complete measurement iff  $m_j = e^{\sigma(j)}$  where  $\sigma(j)$  is a permutation of  $(1, \dots, d)$ . On the other hand, in quantum systems, a complete measurement is given by a rank-one PVM measurement. This follows from Proposition 14 and the fact that a POVM element is extreme iff it is a projection operator.

By definition,  $\mathcal{M}_{\text{comp}}(\mathcal{S}) \subset \mathcal{M}_{\text{ind}}(\mathcal{S})$ . However, the existence of the complete measurements does not necessarily hold for any GPT (See Appendix B for a counter example).

## VI. SOME QUANTITIES RELATED TO AN ENTROPY

In this section, we consider three quantities on  $\mathcal{S}$  in any GPT which are related to the notion of entropy. Indeed, all of them coincides with the Shannon entropy  $H$  and von Neumann entropy  $S$  in classical and quantum systems, respectively, and therefore give generalizations of entropies in classical and quantum systems. However, as is shown, they do not coincide in some GPTs, and does not satisfy some of properties of an entropy. In the following, let  $H(\mathbf{p})$ , or simply as  $H(p_i)$ , denote the Shannon entropy for a probability distribution  $\mathbf{p} = (p_1, \dots, p_d)$ :  $H(\mathbf{p}) := -\sum_i p_i \log p_i$ . We also denote it by  $H(X)$  when the random variable  $X$  are dealt with. The mutual information for a random variable  $X$  and  $J$  are denoted by  $H(X : J) := H(X) + H(J) - H(X, J)$ . In quantum systems, the von Neumann entropy for a density operator  $\rho$  on  $\mathcal{H}$  is denoted by  $S(\rho) := -\text{tr}(\rho \log \rho)$ .

Let us consider a general GPT with a state space  $\mathcal{S}$ . For any state  $s \in \mathcal{S}$ , we denote by  $\mathcal{D}(s)$  the set of all the ensembles  $\{p_x; s_x\}_x$  ( $s_x \in \mathcal{S}, p_x \geq 0, \sum_x p_x = 1$ ) such that  $s = \sum_x p_x s_x$ . The set of all the ensembles for  $s$  with respect to pure states are denoted by  $\mathcal{P}(s) \subset \mathcal{D}(s)$ ; i.e.,  $\{p_x; s_x\} \in \mathcal{P}(s) \Leftrightarrow s = \sum_x p_x s_x, s_x \in \mathcal{S}_{\text{pure}}$ . Note that  $H$  and  $S$  have a concavity property. Both  $H$  and  $S$  are positive and take the minimum value 0 iff the state is pure. The following upper bound of von Neumann

entropy is also well known: for a probability distribution  $(p_i)_i$  and a set of density operators  $\{\rho_i\}_i$ ,

$$S\left(\sum_i p_i \rho_i\right) \leq H(p_i) + \sum_i p_i S(\rho_i), \quad (10)$$

with equality iff density operators  $\rho_i$  are orthogonal to each other. See, for instance [25], for the properties of Shannon and von Neumann entropies.

In any GPT, let us define the following quantities for  $s \in \mathcal{S}$ :

$$S_1(s) := \inf_{M=(m_j)_j \in \mathcal{M}_{\text{ind}}} H(m_j(s)). \quad (11)$$

$$S_2(s) := \sup_{\{p_x, s_x\} \in \mathcal{P}(s)} \sup_{M=(m_j)_j \in \mathcal{M}_{\text{ind}}} H(X : J). \quad (12)$$

$$S_3(s) := \inf_{\{p_x, s_x\} \in \mathcal{P}(s)} H(p_x). \quad (13)$$

In  $S_2(s)$ ,  $H(X : J)$  is defined by a joint distribution  $p_x m_j(s_x)$  with an ensemble  $\{p_x, s_x\} \in \mathcal{P}(s)$  and a measurement  $M = (m_j)_j$ . From the definition and the positivity of the Shannon entropy and the mutual information, the positivity of  $S_1, S_2, S_3$  are obvious. It is easy to see that  $S_2$  can be redefined with respect to  $\mathcal{D}(s)$  and  $\mathcal{M}$ :

**Lemma 5** *We have*

$$S_2(s) = \sup_{\{p_x, s_x\} \in \mathcal{D}(s)} \sup_{M=(m_j)_j \in \mathcal{M}} H(X : J)$$

**Proof** A straightforward computation shows that, for any  $\{p_x, s_x\} \in \mathcal{D}(s)$  and  $M = (m_j)_j \in \mathcal{M}$ , the value of  $H(X : J)$  is not decreased by replacing  $\{p_x, s_x\}$  with the pure state decomposition of  $s$  obtained by decomposing every  $s_x$  into pure states, and by replacing  $M$  with the indecomposable measurement obtained by decomposing every  $m_j$  into indecomposable effects (cf. Proposition 11). This implies the desired relation. ■

However, note that it is essential to use  $\mathcal{M}_{\text{ind}}$  and  $\mathcal{P}(s)$  for the definitions of  $S_1$  and  $S_3$ . Indeed, redefinitions of  $S_1$  and  $S_3$  with respect to  $\mathcal{D}(s)$  and  $\mathcal{M}$  give trivial quantities:  $\inf_{M \in \mathcal{M}} H(m_j(s)) = 0$ ,  $\inf_{\{p_x, s_x\} \in \mathcal{D}(s)} H(\{p_x\}_x) = 0$ .

Notice that all three quantities (11)-(13) are defined with physical languages:  $S_1(s)$  measures the minimum uncertainty of measurement among indecomposable measurements under a state  $s$ ;  $S_2(s)$  measures the maximum accessible information (by an optimal measurement) among any preparation of  $s$  (See below). Finally,  $S_3(s)$  measures the minimum uncertainty for a preparation of  $s$  with respect to pure states.

Indeed, under the preparation of states  $s_x$  with a prior probability distribution  $p_x$ , the accessible information  $I(\{p_x, s_x\})$  is defined by  $\sup_{M=(m_j)_j \in \mathcal{M}} H(X : J)$  where the joint probability distribution between  $X$  and  $J$  (measurement outcome by a measurement  $M = (m_j)_j$ ) is given by  $p(x, j) := p_x m_j(s_x)$ . Therefore, from Lemma 5, we have  $S_2(s) = \sup_{\{p_x, s_x\} \in \mathcal{D}(s)} I(\{p_x, s_x\})$ , and thus



**Proposition 17** *In GPT, for any preparation of states  $\{p_x, s_x\}$ , the accessible information is bounded as*

$$I(\{p_x, s_x\}) \leq S_2(s), \quad (14)$$

where  $s := \sum_x p_x s_x$ .

Notice that, in quantum systems, the Holevo bound [27] gives an upper bound of the accessible information by the Holevo  $\chi$  quantity: For a preparation of density operators  $\rho_x$  with a probability distribution  $p_x$ ,

$$I(\{p_x, \rho_x\}) \leq \chi := S(\rho) - \sum_x p_x S(\rho_x). \quad (15)$$

In the following, we see that  $S_2$  coincides with the von Neumann entropy in quantum systems. Thus, (14) gives a looser bound than the Holevo bound in quantum systems. (For the pure state ensemble, (14) gives exactly the Holevo bound since the von Neumann entropy vanishes on pure states.)

Now, we show that all three quantities (11)-(13) are generalizations of Shannon and von Neumann entropies in classical and quantum systems:

**Theorem 3** (i) *In classical systems,  $S_1(s), S_2(s), S_3(s)$  are the Shannon entropy.* (ii) *In quantum systems,  $S_1(s), S_2(s), S_3(s)$  are the von Neumann entropy.*

**Proof** (i) Let  $\mathcal{S}_c$  be the state space of a classical system. From Proposition 13, any indecomposable measurement in classical system is given by  $(\lambda_{i,\mu} e^{(\mu)})_{i,\mu}$  where  $\lambda_{i,\mu} \geq 0, \sum_i \lambda_{i,\mu} = 1$  for any  $\mu = 1, \dots, d$ . Thus, for a state  $\mathbf{p} = (p_1, \dots, p_d) \in \mathcal{S}_c$ , the probability distribution given by the indecomposable measurement is  $(\lambda_{i,\mu} p_\mu)_{i,\mu}$ . Note that from the concavity of the function  $g(x) := -x \log x$  ( $x \in [0, 1]$ ) with the convention  $g(0) = 0$ , it holds that  $g(\lambda x) \geq \lambda g(x)$ , and thus we have  $H(\lambda_{i,\mu} p_\mu) = \sum_{i,\mu} g(\lambda_{i,\mu} p_\mu) \geq \sum_\mu (\sum_i \lambda_{i,\mu}) g(p_\mu) = H(p_\mu)$ . Thus, we have  $S_1(\mathbf{p}) \geq H(\mathbf{p})$ . Since  $(e^{(\mu)})_\mu$  is an indecomposable measurement with which the probability distribution is given by  $\mathbf{p}$ , we have  $S_1(\mathbf{p}) = H(\mathbf{p})$ .

As mentioned before, a state space of a classical system is characterized by a simplex. Thus, we have

$$S_2(\mathbf{p}) = \sup_{M \in \mathcal{M}} H(X : J)$$

where the random variable  $X$  is described by the probability distribution  $\mathbf{p}$ . Remind that the mutual information can be written as  $H(X : J) = H(X) - H(X|J)$  where  $H(X|J)$  denotes the conditional entropy, and it follows that

$$S_2(\mathbf{p}) = \sup_{M \in \mathcal{M}} H(X : J) = H(X) - \inf_{M \in \mathcal{M}} H(X|J).$$

Since there exists a measurement  $M = (m_j)$  to discriminate all pure states in a classical system, we have  $\inf_{M \in \mathcal{M}} H(X|J) = 0$  (i.e., the uncertainty of  $X$  conditioned on the information of  $J$  is zero). Therefore, we have  $S_2(\mathbf{p}) = H(X) = H(\mathbf{p})$ .

Again from the unique pure state decomposition, there exists the unique ensemble  $\{p_\mu, p^{(\mu)}\}_{\mu=1}^d$  for any state  $\mathbf{p} = (p_1, \dots, p_d) \in \mathcal{S}_c$ . Therefore, we have  $S_3(\mathbf{p}) = H(\mathbf{p})$ .

(ii) Next, we consider a quantum system described by a Hilbert space  $\mathcal{H}$ . First, let  $f$  be a concave function on  $[0, 1]$  such that  $f(0) = 0$ , and let  $\rho$  be a density operator on  $\mathcal{H}$ . Then, it is easy to show [35] that for all vector  $\psi \in \mathcal{H}$  such that  $\|\psi\| \leq 1$ , we have

$$f(\langle \psi | \rho | \psi \rangle) \geq \langle \psi | f(\rho) | \psi \rangle.$$

Let us fix any indecomposable POVM measurement  $(E_j)_j$  on quantum system  $\mathcal{H}$ , i.e., rank-one POVM measurement. We can write  $E_j = |\psi_j\rangle\langle\psi_j|$  with a vector  $\psi \in \mathcal{H}$  such that  $0 < \|\psi_j\| \leq 1$  and  $\sum_i |\psi_j\rangle\langle\psi_j| = \mathbb{I}$ . Remind that the von Neumann entropy of  $\rho$  is defined by

$$S(\rho) := \text{tr } g(\rho)$$

with the concave function  $g(x) := -x \log x$  with the convention  $g(0) = 0$ . Applying  $g$  to the above concave function  $f$ , we have  $H(e_j(\rho)) = \sum_j g(\langle \psi_j | \rho | \psi_j \rangle) \geq \sum_j \langle \psi_j | g(\rho) | \psi_j \rangle = \text{tr}(g(\rho) \sum_i E_i) = \text{tr } g(\rho) = S(\rho)$ . By considering the indecomposable measurement given by  $(|\phi_j\rangle\langle\phi_j|)_j$  where  $\phi_j$ s are complete eigenvectors of  $\rho$ , we obtain  $S_1(\rho) = S(\rho)$ .

Next, from the Holevo bound (15), we have

$$S_2(\rho) \leq S(\rho) - \inf_{\{p_x, \rho_x\} \in \mathcal{D}(\rho)} \left( \sum_x p_x S(\rho_x) \right) = S(\rho).$$

The final equality follows from the eigenvalue decomposition  $\rho = \sum_x p_x |\phi_x\rangle\langle\phi_x|$  and  $S(|\phi_x\rangle\langle\phi_x|) = 0$ . Again with the decomposition  $\{p_x, \rho_x = |\phi_x\rangle\langle\phi_x|\}$  of eigenvalues and eigenvectors, there exists an optimal measurement  $M_j := |\phi_j\rangle\langle\phi_j|$  to discriminate  $\rho_x$ , and thus one has  $H(X : J) = H(\mathbf{p})$ . Since  $S(\rho) = H(\mathbf{p})$ , we have  $S(\rho) = H(X : J) \leq S_2(\rho)$ .

Finally, let  $\{p_x, \rho_x\} \in \mathcal{P}(\rho)$  be a pure state decomposition of  $\rho$ . Then, from the inequality (10) and the fact that  $S(\rho_x) = 0$  for pure states  $\rho_x$ , we have

$$S(\rho) \leq H(\{p_x\}) \leq S_3(\rho).$$

Moreover, an eigenvalue decomposition  $\rho = \sum_x p_x |\phi_x\rangle\langle\phi_x|$  of  $\rho$  gives a pure state decomposition such that  $\rho_x = |\phi_x\rangle\langle\phi_x|$  are orthogonal to each other, we have the equality:  $S_3(\rho) = S(\rho)$ . This completes the proof. ■

Notice that the fact that  $S_1, S_2, S_3$  coincide with the von Neumann entropy in quantum systems shows that we have alternative expressions with operational meanings for the von Neumann entropy. The characterization of  $S$  by  $S_3$  has been noticed by Jaynes [28]. Here, we remark that  $S_1$  could be defined by the infimum of Shannon entropy among not indecomposable measurements but complete measurements. Then, it is easy to restate the above mentioned proof to show  $S_1$  coincides with Shannon and von Neumann entropy in classical and quantum

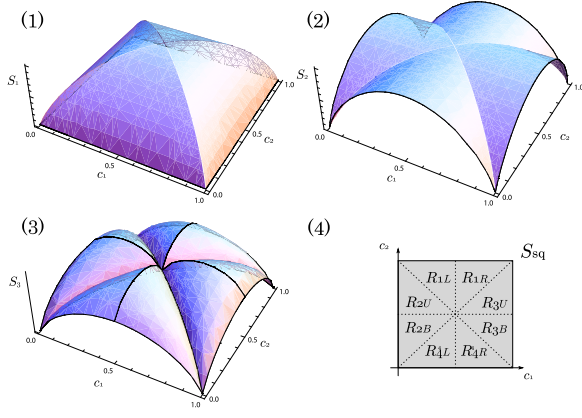


FIG. 1: In the squared systems, (1), (2) and (3) show the graphs of  $S_1$ ,  $S_2$  and  $S_3$ . (4) specifies the region  $R_{1L}, \dots, R_{4R}$ .

systems. However, as we have noticed in Sec. VB, there exists a GPT where no complete measurements exists. This is the reason why we have defined  $S_1$  among indecomposable measurements.

In order to see the properties of  $S_1, S_2, S_3$  in a general GPT, let us again consider the squared system  $\mathcal{S}_{\text{sq}}$ . Let  $h(x) := -x \log x - (1-x) \log(1-x)$  is the binary Shannon entropy:

**Proposition 18** *In the squared system, for  $s = (c_1, c_2) \in \mathcal{S}_{\text{sq}}$ , we have*

$$S_1(s) = \min[h(c_1), h(c_2)], \quad (16)$$

$$S_2(s) = \max[h(c_1), h(c_2)], \quad (17)$$

$$S_3(s) = \begin{cases} k(c_1 + c_2 - 1) & s \in R_{1L} \\ k(c_1) & s \in R_{1R} \\ k(0) & s \in R_{2U} \\ k(c_1) & s \in R_{2B} \\ k(c_2) & s \in R_{3U} \\ k(c_2) & s \in R_{3B} \\ k(c_1 + c_2 - 1) & s \in R_{4L} \\ k(c_2) & s \in R_{4R} \\ k(0) & s \in R_{4R'} \end{cases} \quad (18)$$

where  $k(x) := H(\{x, c_1 - x, c_2 - x, 1 + x - c_1 - c_2\})$  and the regions  $R_{1L}, \dots, R_{4R} \subset \mathcal{S}_{\text{sq}}$  are given in Fig. 1-(4).

(See Appendix A for the proof.) See graphs of  $S_1, S_2$  and  $S_3$  in Fig. 1-(1)-(3). Moreover, in  $\mathcal{S}_{\text{sq}}$ , the following relations among  $S_1, S_2$  and  $S_3$  are true:

**Proposition 19** *For any  $s \in \mathcal{S}_{\text{sq}}$ ,*

$$S_1(s) \leq S_2(s) \leq S_3(s)$$

(See Appendix A for the proof.)

## A. Concavity

In this section, we consider the concavity properties of  $S_1, S_2$  and  $S_3$ . It turns out that  $S_1$  is concave on  $\mathcal{S}$  in any GPT, while there exists GPT models where  $S_2$  and  $S_3$  are not concave.

**Proposition 20** *In any GPT,  $S_1$  is concave on  $\mathcal{S}$ .*

**Proof** Let  $(p_x)_x$  ( $x = 1, \dots, m$ ) be a probability distribution and let  $s_x \in \mathcal{S}$  ( $x = 1, \dots, m$ ). Then, from the affinity of effects  $m_j$  and the concavity of the Shannon entropy, we have

$$\begin{aligned} S_1\left(\sum_x p_x s_x\right) &= \inf_{M=(m_j)_j \in \mathcal{M}_{\text{ind}}} H(e_j(\sum_x p_x s_x)) \\ &\geq \inf_{M=(m_j)_j \in \mathcal{M}_{\text{ind}}} \sum_x p_x H(m_j(s_x)) \\ &\geq \sum_x p_x \inf_{M=(m_j)_j \in \mathcal{M}_{\text{ind}}} H(m_j(s_x)) \\ &= \sum_x p_x S_1(s_x). \end{aligned} \quad (19)$$

■

Contrast to  $S_1$ ,  $S_2$  and  $S_3$  does not satisfy the concavity in some GPT. It is easy to give counter examples but it is obvious that concavity does not hold in the squared systems from the Fig. 1-(2) and (3).

In stead of the concavity, we show the following:  $S_2$  satisfies the following *weak concavities*:

**Proposition 21** *(Weak Concavity) In any GPT,  $S_2$  satisfies the followings:*

$$S_2\left(\sum_x p_x s_x\right) \geq \frac{\sum_x p_x^2 S_2^2(s_x)}{\sum_x p_x S_2(s_x)}, \quad (20)$$

$$S_2\left(\sum_x p_x s_x\right) \geq \sum_x p_x^2 S_2(s_x), \quad (21)$$

$$S_2\left(\sum_x p_x s_x\right) \geq \frac{1}{|X|} \sum_x p_x S_2(s_x), \quad (22)$$

$$S_2\left(\sum_x p_x s_x\right) \geq \max_x p_x S_2(s_x), \quad (23)$$

for any  $\{p_x, s_x\}_{x \in X} \in \mathcal{D}(s)$  (in (20), we interpret the right-hand side as 0 if  $S_2(p_x)$  are all 0).

**Proof** To prove this proposition, we use the following lemma (see Appendix A for the proof):

**Lemma 6** *Let  $\{p_x, s_x\}_{x \in X} \in \mathcal{D}(s)$ ,  $p_x \neq 0$ . Then for any value  $\pi_x \geq 0$ ,  $x \in X$  such that  $\sum_x \pi_x = 1$ , we have*

$$S_2\left(\sum_x p_x s_x\right) \geq \sum_x \pi_x p_x S_2(s_x).$$

By using this lemma, (20) is proved by putting  $\pi_x = p_x S_2(s_x) / (\sum_{x'} p_{x'} S_2(s_{x'}))$  (here we may assume that the denominator of the  $\pi_x$  is nonzero, as otherwise the claim

is obvious); (21) is proved by putting  $\pi_x = p_x$ ; (22) is proved by putting  $\pi_x = 1/|X|$ ; and (23) is proved by putting  $\pi_x = \delta_{xx_0}$  where  $x_0 \in X$  is such that  $p_{x_0}S_2(s_{x_0}) = \max_x p_x S_2(s_x)$ . ■

**Proposition 22** *In any GPT,  $S_3$  satisfies*

$$S_3\left(\sum_{i=1}^m p_i s_i\right) \leq H(p_i) + \sum_{i=1}^m p_i S_3(s_i),$$

for any  $s_i \in \mathcal{S}$  ( $i = 1, \dots, m$ ) and probability distribution  $(p_i)_{i=1}^m$ .

**Proof** Let  $\epsilon > 0$  be an arbitrary positive number. Let  $s := \sum_{i=1}^m p_i s_i$  and let  $\{p_j^i; s_j^i\}_j \in \mathcal{P}(s_i)$  be an “optimal” decomposition of  $s_i$  such that  $S_3(s_i) + \epsilon \geq H(p_j^i)$ . Since  $\{p_i p_j^i\}_{i,j} \in \mathcal{P}(s)$ , we have  $S_3(s) \leq H(I, J) := -\sum_{i,j} p_i p_j^i \log(p_i p_j^i) = -\sum_i p_i \log p_i + \sum_i p_i (-\sum_j p_j^i \log p_j^i) = H(p_x) + \sum_i p_i H(p_j^i) \leq H(p_x) + \sum_i p_i S_3(s_i) + \epsilon$ . ■

Thus,  $S_3$  satisfies the same upper bound (10) of the von Neumann entropy in any GPT.

## B. Measure for pureness

Since both the Shannon entropy and the von Neumann entropy vanishes if and only if the state is pure, they can be considered as a measure of pureness. (Note also that they take the maximum value iff the state is the maximal mixed states.) We show that  $S_2$  and  $S_3$  has this desired property in any GPT, while  $S_1$  does not satisfy this in general.

**Proposition 23** *In any GPT, (i)  $S_2(s) = 0$  if and only if  $s$  is pure. (ii)  $S_3(s) = 0$  if and only if  $s$  is pure.*

**Proof** (i) Let  $s \in \mathcal{S}$  be a pure state. Since  $s$  is an extreme point of  $\mathcal{S}$ ,  $\mathcal{P}(s)$  has essentially the unique (trivial) decomposition:  $\{1; s\}$  with  $H(X) = 0$ . Thus, we have

$$S_2(s) = \sup_{M=(m_j)_j \in \mathcal{M}} H(X : J) = -\inf_M H(X|J) \leq 0.$$

To see the converse, let  $S_2(s) = 0$  for  $s \in \mathcal{S}$  and let  $s = p_1 s_1 + p_2 s_2$  where  $p_1 \in (0, 1)$ ,  $p_1 + p_2 = 1$  and  $s_1, s_2 \in \mathcal{S}$ . Since  $S_2(s) = 0$  and  $\{p_x; s_x\}_{x=1,2} \in D(s)$ , we have

$$H(X : J) = 0$$

for the random variable  $X = 1, 2$  and for any  $M = (m_j) \in \mathcal{M}$ . This implies that the joint probability  $p(x, j) := p_x m_j(s_x)$  is a product state, or equivalently, the conditional probability  $p(j|x) := p(x, j)/p_x = m_j(s_x)$  is independent of  $x$  (Notice that  $p_1, p_2 \neq 0$ ). In particular, we have  $m_j(s_1) = p(j|1) = p(j|2) = m_j(s_2)$ . Since this holds for any effect  $m_j$ , we have  $s_1 = s_2$  from the separating property of states. Therefore,  $s$  has only the trivial decomposition and is a pure state.

(ii) Let  $s \in \mathcal{S}$  be a pure state and thus  $\mathcal{P}(s)$  has essentially the unique (trivial) decomposition:  $\{1; s\}$  where  $H(X) = 0$ . Thus, we have  $S_3(s) = H(X) = 0$ . Conversely, let  $S_3(s) = 0$ . Then, for any  $\{p_x; s_x\}_x \in \mathcal{P}(s)$ , it follows  $H(X) = 0$ . Assume that  $s$  is not a pure state. Then, we have  $\{p_x, s_x\}_X \in \mathcal{P}(s)$  where  $p_{x_1}, p_{x_2} > 0$  for some  $x_1, x_2 \in X$ . However, this contradicts that  $H(X) = 0$ . Therefore,  $s$  is a pure state. ■

Contrast to  $S_2$  and  $S_3$ ,  $S_1$  does not satisfy this property. For instance, from (16),  $S_1(s) = 0$  for any state  $s$  on the boundary (four edges) of  $\mathcal{S}_{\text{sq}}$ . (See Fig. 1-(1). Note that  $s$  on edges but not on vertexes is not a pure state.) In general GPT, we show the followings:

**Proposition 24** *In any GPT,  $S_1(s) = 0$  implies that  $s$  is on the boundary of  $\mathcal{S}$ .*

**Proof** It suffices to consider the case that  $\mathcal{S}$  has at least two states. To prove this proposition, we use the following two lemmas (see Appendix A for the proofs):

**Lemma 7** *Let  $k, \ell \geq 1$  be an integer. Let  $h(x) = -x \log x$ . If  $x_1, \dots, x_\ell \in [0, 1/k]$  and  $\sum_j x_j = 1$ , then  $H(x) = \sum_j h(x_j) \geq \log k$ .*

**Lemma 8** *For any  $s \in \mathcal{S}$ , the map  $f_s : \mathcal{E}(\mathcal{S}) \times \mathcal{S} \rightarrow \mathbb{R}$ ,  $f_s(e, t) = e(s) - e(t)$ , is continuous.*

Let  $s \in \mathcal{S}$  such that  $S_1(s) = 0$ . First we show that  $\sup_{(e,t)} f_s(e, t) = 1$ . Let  $k \geq 2$  be any integer. Since  $S_1(s) = 0$ , there is an indecomposable measurement  $M = (m_i)_i \in \mathcal{M}_{\text{ind}}$  such that  $H(m_i(s)) < h(1/k)$  ( $< \log k$ ). Then we have  $m_i(s) \geq 1 - 1/k$  for some  $i$ , as otherwise we have a contradiction as follows: If  $m_{i_0}(s) \in (1/k, 1 - 1/k)$  for some  $i_0$  then we have  $H(m_{i_0}(s)) \geq h(m_{i_0}(s)) > h(1/k)$ ; while if  $m_i(s) \leq 1/k$  for all  $i$  then we have  $H(m_i(s)) \geq \log k$  by Lemma 7. For this  $m_i$ , Lemma 4 implies that there is a state  $t \in \mathcal{S}$  such that  $m_i(t) = 0$ . This implies that  $f_s(m_i, t) \geq 1 - 1/k$ . Since  $k \geq 2$  is arbitrary, we have  $\sup_{(e,t)} f_s(e, t) = 1$ . Since  $\mathcal{E}(\mathcal{S}) \times \mathcal{S}$  is compact, Lemma 8 implies that  $f_s(e, t) = 1$  for some  $e \in \mathcal{E}(\mathcal{S})$  and  $t \in \mathcal{S}$ , therefore  $e(s) = 1$  and  $e(t) = 0$ . This implies that  $e$  is not constant and  $s$  lies in a supporting hyperplane of  $\mathcal{S}$ , hence  $s$  is on the boundary of  $\mathcal{S}$  as desired. ■

Note that, in  $\mathcal{S}_{\text{sq}}$ , the converse is also true: all states on the boundary  $s$  satisfy  $S_1(s) = 0$ . However, this is not the case for any GPT. In particular, one can construct a GPT where  $S_1(s) \neq 0$  even for a pure state  $s$ . For instance, consider a GPT introduced in Appendix B with state space  $\mathcal{S} \subset \mathbb{R}^2$ , which has the four pure states  $(0, 0)$ ,  $(1, 0)$ ,  $(0, 1)$ , and  $(2, 2)$ . Then any indecomposable effect in  $\mathcal{S}$  is of the form  $\lambda e_i$  such that  $0 < \lambda \leq 1$  and  $e_i$  is one of the four effects in Table II in Appendix B. This implies that for any indecomposable measurement  $M = (m_i)_i \in \mathcal{M}_{\text{ind}}$  we have  $m_i(0, 0) \leq 2/3$  for all  $i$ , therefore  $S_1(0, 0) > 0$  (see Lemma 7). Thus, in general GPT, neither directions of “ $s$  is pure  $\Leftrightarrow S_1(s) = 0$ ” does not holds in general. In the next section, we consider a class of GPTs with fairly fine property.

## VII. PRINCIPLE OF EQUALITY FOR PURE STATES AND SYMMETRIC GPT

In the last part of the preceding section, we considered a GPT where for some pure state  $s$  it holds that  $S_1(s) > 0$  (See GPT in Appendix B). However, the structure of state space are asymmetric and might be just toy models for GPTs. On the other hand, both classical and quantum systems has a certain class of symmetric structures: In particular, there are no special pure states which have different properties from another pure states. We call this the principle of *equality for pure states* and can be formulated as follows:

**Definition 4** (*Equality for pure states*) *We say that GPT satisfy the principle of equality for pure states if, for any pure states  $s_1, s_2 \in \mathcal{S}$ , there exists a bijective affine map  $f$  on  $\mathcal{S}$  such that  $s_2 = f(s_1)$ . We call a GPT satisfying this property a symmetric GPT.*

It is easy to see that:

**Proposition 25** *Classical, quantum, and hyper cuboid systems are all symmetric.*

In particular, notice that, in quantum systems for any pure states  $\rho_1 = |\psi_1\rangle\langle\psi_1|, \rho_2 = |\psi_2\rangle\langle\psi_2|$ , there exists a unitary operator  $U$  such that  $\rho_2 = U\rho_1U^\dagger$ .

We show that  $S_1$  vanishes for any pure states in a symmetric GPT. To see this, we first show:

**Lemma 9** *In any GPT, there exists a pure state  $s$  such that  $S_1(s) = 0$ .*

**Proof** Let  $e_1$  be an indecomposable and pure effect (see Proposition 12), and let  $u - e_1 = e_2 + \dots + e_m$  be an indecomposable decomposition of  $u - e_1$  (see Proposition 11). Then,  $M = (e_j)_{j=1}^m$  is an indecomposable measurement. From Proposition 10, there exists a pure state  $s$  such that  $e_1(s) = 1$ . Thus, we have  $H(e_j(s)) = 0$ , and  $S_1(s) = 0$ . ■

**Proposition 26** *Let  $\mathcal{S}$  be the state space of a symmetric GPT. Then,  $S_1(s) = 0$  for any pure state  $s$ .*

**Proof** From Lemma 9, there exists a pure state  $s_0$  such that  $S_1(s_0) = 0$ . For any pure state  $s$ , there exists a bijective affine  $f$  such that  $s_0 = f(s)$ . Let  $M = (m_j)_j$  be an indecomposable measurement such that  $H(m_j(s_0)) = 0$ . Then, it is easy to see that  $\tilde{M} := (\tilde{m}_j)_j$  where  $\tilde{m}_j := m_j \circ f$  is an indecomposable measurement. Therefore, it follows that  $H(\tilde{m}_j(s)) = H(m_j(s_0)) = 0$ . Thus, we have proved that  $S_1(s) = 0$  for any pure state  $s$ . ■

Therefore, in a symmetric GPT,  $S_1$  measures a pureness in some sense. However, as the squared GPT shows, the converse of Proposition 26 does not holds in general even among symmetric GPTs.

## VIII. CONCLUDING REMARKS

We have discussed some distinguishability measures (especially, Kolmogorov distance and fidelity) in any GPT. In a similar way of quantum information theory, it will be convenient to use these measures in constructing an information theory in GPT. Indeed, we have reformulated no-cloning theorem and information-disturbance theorem using fidelity.

We have also proposed and investigated three quantities related to entropies in any GPT. All of them are generalizations of Shannon and von Neumann entropy in classical and quantum systems, respectively. However, they are in general distinct quantities, as the squared system gives the example. The concavity of  $S_1$  in any GPT holds while it breaks for  $S_2$  and  $S_3$  in some GPT.  $S_2$  and  $S_3$  provides a measure for pureness, while  $S_1$  does not. However, in a symmetric GPT which satisfies the principle of *equality of pure states*, it follows that  $S_1(s) = 0$  for any pure states  $s$ . In the attempt to find principles of our world, which is described by a quantum system at least for the present, we think that symmetric GPTs are enough to consider by assuming the principle of equality for pure states. However, let us remark here that both classical and quantum systems satisfy stronger principle, which we call *strong equality for pure states* or *equality for distinguishable pure states* which can be formulated as follows:

**Definition 5** (*Strong equality for pure states*) *We say that GPT satisfies the principle of strong equality for pure states if it satisfies the following: Let  $\{s_i \in \mathcal{S}_{\text{pure}}\}_{i=1}^n$  and  $\{t_i \in \mathcal{S}_{\text{pure}}\}_{i=1}^m$  (let  $n \geq m$ ) be two distinguishable sets of pure states, i.e., there exists a measurement  $M = (m_i)_i$  ( $N = (n_i)_i$ ) such that  $m_i(s_j) = \delta_{ij}$  ( $n_i(t_j) = \delta_{ij}$ ). Then, there exists a bijective affine map  $f$  on  $\mathcal{S}$  such that  $t_i = f(s_i)$  ( $i = 1, \dots, m$ ).*

Notice that the squared GPT is symmetric but does not satisfies this strong equality for pure states. (For instance, consider  $\{(0,0), (0,1)\}$  and  $\{(0,0), (1,1)\}$ .) It might be interesting to consider these kind of stronger conditions which classical and quantum systems satisfy. In particular, we don't know any principles which makes the converse of Proposition 26 to hold.

**Acknowledgment** We would like to thank useful comments and discussions with Dr. Imafuku and Dr. Miyadera. Part of this work is supported by Grant-in-Aid for Young Scientists (B), The Ministry of Education, Culture, Sports, Science and Technology (MEXT) (No.20700017).

*Note added.* Related but independent works for *entropies* in GPT has appeared recently in Ref. [31, 32] while completing this paper. We will continuously see the relations between our work and the results there in near future.



## APPENDIX A: PROOFS OF SOME PROPOSITIONS

**[Proof of Proposition 2]** Notice that for any measurement  $M = \{m_i\} \in \mathcal{M}(\mathcal{S}')$ , and any affine map  $\Lambda \in \mathcal{A}(\mathcal{S}, \mathcal{S}')$ , we have another measurement  $N = \{n_i\} \in \mathcal{M}(\mathcal{S})$  where  $n_i := m_i \circ \Lambda$ . Let  $M = \{m_i\} \in \mathcal{M}(\mathcal{S}')$  be an optimal measurement which attains the maximum:

$$D(\Lambda(s_1), \Lambda(s_2)) = \frac{1}{2} \sum_i |m_i(\Lambda(s_1)) - m_i(\Lambda(s_2))|.$$

Then, we have

$$D(\Lambda(s_1), \Lambda(s_2)) = \frac{1}{2} \sum_i |n_i(s_1) - n_i(s_2)| \leq D(s_1, s_2).$$

**[Proof of Proposition 3]** Let  $M = \{m_i\} \in \mathcal{M}$  be a measurement which satisfies

$$D\left(\sum_i p_i s_i, \sum_i q_i t_i\right) = \frac{1}{2} \sum_i |m_i(\sum_j p_j s_j) - m_i(\sum_j q_j t_j)|.$$

Then, we have

$$\begin{aligned} D\left(\sum_i p_i s_i, \sum_i q_i t_i\right) &= \frac{1}{2} \sum_i \left| \sum_j p_j m_i(s_j) - \sum_j q_j m_i(t_j) \right| \\ &\leq \frac{1}{2} \sum_{i,j} p_j |(m_i(s_j) - m_i(t_j))| + \frac{1}{2} \sum_{i,j} |(p_j - q_j)| m_i(t_j) \\ &\leq \sum_j p_j D(s, t) + D_c(p_i, q_i), \end{aligned}$$

where we have used (i) affinity of  $m_i$ , (ii) triangle inequality of  $|\cdot|$ , and (iii)  $\sum_i m_i = u$ . ■

**[Proof of Proposition 4]** The proof goes almost similar manner with that of Proposition 2, only noting a technical treatment of the infimum: For any  $\epsilon > 0$ , there exists an “optimal” measurement  $M = (m_j)_j$  such that  $F(\Lambda(s_1), \Lambda(s_2)) + \epsilon \geq \sum_j \sqrt{m_j(\Lambda(s_1))m_j(\Lambda(s_2))}$  from the definition of the fidelity. By using a measurement  $N = (n_i)_i$  where  $n_i := m_i \circ \Lambda$ , it follows that  $F(\Lambda(s_1), \Lambda(s_2)) + \epsilon \geq \sum_j \sqrt{n_j(s_1)n_j(s_2)} \geq F(s_1, s_2)$ . Since  $\epsilon > 0$  is arbitrary, we obtain the monotonicity. ■

**[Proof of Proposition 5]** For any  $\epsilon > 0$ , let  $M = (m_i)_i$  be an “optimal” measurement satisfying

$$F\left(\sum_i p_i s_i, \sum_i q_i t_i\right) + \epsilon \geq \sum_k \sqrt{m_k\left(\sum_i p_i s_i\right)m_k\left(\sum_j q_j t_j\right)}.$$

Using the affinity of  $m_i$  and the Schwarz inequality between vectors  $(\sqrt{p_i m_k(s_i)})_i$  and  $(\sqrt{q_i m_k(t_i)})_i$ , one gets

$$\begin{aligned} &F\left(\sum_i p_i s_i, \sum_i q_i t_i\right) + \epsilon \\ &\geq \sum_k \sqrt{\sum_i p_i m_k(s_i)} \sqrt{\sum_j q_j m_k(t_j)} \\ &\geq \sum_k \sum_i \sqrt{p_i m_k(s_i) q_i m_k(t_i)} \geq \sum_i \sqrt{p_i q_i} F(s_i, t_i). \end{aligned}$$

Letting  $\epsilon \rightarrow 0$ , we obtain the strong concavity. ■

**[Proof of Proposition 6]** (i) For any  $\epsilon > 0$ , let  $M = (m_i)_i \in \mathcal{M}(\mathcal{S}_A)$  and  $N = (n_j)_j \in \mathcal{M}(\mathcal{S}_B)$  be “optimal” measurements such that  $F(s_1, s_2) + \epsilon \geq \sum_i \sqrt{m_i(s_1)m_i(s_2)}$  and  $F(t_1, t_2) + \epsilon \geq \sum_j \sqrt{n_j(t_1)n_j(t_2)}$ , respectively. Then,  $g_{ij} = m_i \otimes n_j \in \mathcal{E}(\mathcal{S}_A \otimes \mathcal{S}_B)$  gives a (joint) measurement  $G = (g_{ij})_{ij} \in \mathcal{M}(\mathcal{S}_A \otimes \mathcal{S}_B)$ , and  $(F(s_1, s_2) + \epsilon)(F(t_1, t_2) + \epsilon) \geq \sum_{ij} \sqrt{g_{ij}(s_1 \otimes t_1)g_{ij}(s_2 \otimes t_2)} \geq F(s_1 \otimes t_1, s_2 \otimes t_2)$ .

(ii) For any  $\epsilon > 0$ , let  $M = (m_i)_i \in \mathcal{S}_A$  be an “optimal” measurement such that  $F(s_A, t_A) + \epsilon \geq \sum_i \sqrt{m_i(s_A)m_i(t_A)}$ . By noting that  $g_i = m_i \otimes u_B$  gives a measurement on  $\mathcal{S}_A \otimes \mathcal{S}_B$  and  $g_i(s) = m_i(s_A)$ ,  $g_i(t) = m_i(t_A)$ , one has  $F(s_A, t_A) + \epsilon \geq \sum_i \sqrt{g_i(s)g_i(t)} \geq F(s, t)$ .

(iii) The inequality  $F(s_1, s_2) \geq F(s_1 \otimes t, s_2 \otimes t) \geq \sum_i \sqrt{m_i(s_1) \otimes m_i(s_2)}$  follows from (i) and  $F(t, t) = 1$ . To see the opposite inequality, let  $G = (g_i)_i \in \mathcal{M}(\mathcal{S}_A \otimes \mathcal{S}_B)$  be an “optimal” measurement such that  $F(s_1 \otimes t, s_2 \otimes t) + \epsilon \geq \sum_i \sqrt{g_i(s_1 \otimes t)g_i(s_2 \otimes t)}$  for any  $\epsilon > 0$ . Then, since  $m_i(s) := g_i(s \otimes t)$  ( $\forall s \in \mathcal{S}_A$ ) gives a measurement  $M = (m_i)_i \in \mathcal{S}_A$ , we have  $F(s_1 \otimes t, s_2 \otimes t) + \epsilon \geq \sum_i \sqrt{m_i(s_1) \otimes m_i(s_2)} \geq F(s_1, s_2)$ . ■

**[Proof of Proposition 7]** The proof is essentially the same as in [24]. For any  $\epsilon > 0$ , let  $M = (m_i)_i$  be an “optimal” measurement which satisfies  $F(s, t) + \epsilon \geq \sum_i \sqrt{p_i q_i}$  where  $p_i := m_i(s)$ ,  $q_i := m_i(t)$ . It follows that  $\sum_i (\sqrt{p_i} - \sqrt{q_i})^2 = \sum_i p_i + \sum_i q_i - 2 \sum_i \sqrt{p_i q_i} \geq 2(1 - F(s, t) - \epsilon)$ . Noting that  $|\sqrt{p_i} - \sqrt{q_i}| \leq |\sqrt{p_i} + \sqrt{q_i}|$ , we have  $\sum_i (\sqrt{p_i} - \sqrt{q_i})^2 = \sum_i |\sqrt{p_i} - \sqrt{q_i}| |\sqrt{p_i} + \sqrt{q_i}| \leq \sum |p_i - q_i| \leq 2D(s, t)$ . Next, let  $N = \{f_i\} \in \mathcal{M}$  be an optimal measurement which satisfies  $D(s, t) = \frac{1}{2} \sum_i |r_i - s_i|$ , where  $r_i = n_i(s)$ ,  $s_i = n_i(t)$ . Then, we have  $D(s, t)^2 = \frac{1}{4} (\sum_i |r_i - s_i|)^2 = \frac{1}{4} (\sum_i |\sqrt{r_i} - \sqrt{s_i}| |\sqrt{r_i} + \sqrt{s_i}|)^2 \leq \frac{1}{4} (\sum_i |\sqrt{r_i} - \sqrt{s_i}|^2) (\sum_i |\sqrt{r_i} + \sqrt{s_i}|^2) = \frac{1}{4} (\sum_i (r_i - \sqrt{r_i} \sqrt{s_i} + s_i)^2) (\sum_i (\sqrt{r_i} + \sqrt{s_i})^2) = \frac{1}{4} (\sum_i r_i + \sum_i s_i - 2 \sum_i \sqrt{r_i s_i}) (\sum_i r_i + \sum_i s_i + 2 \sum_i \sqrt{r_i s_i}) = (1 - \sum_i \sqrt{r_i s_i}) (1 + \sum_i \sqrt{r_i s_i}) = (1 - (\sum_i \sqrt{r_i s_i})^2) \leq 1 - F(s, t)^2$ , where we have used the Schwarz inequality. ■

**[Proof of Proposition 11]** In the proof, we use some terminology from convex geometry. We say that a subset  $C$  of a finite dimensional Euclidean space  $\mathbb{R}^N$  is a *cone* if  $v \in C$  and  $\lambda \geq 0$  imply  $\lambda v \in C$  (hence  $0 \in C$ ). We say that a closed convex cone  $C$  is *pointed* if  $C \cap -C = \{0\}$ . In the proof of Proposition 11, we use the following fact for pointed cones:

**Lemma 10 ([29, Theorem 3.3.15])** *A closed convex cone  $C \subset \mathbb{R}^N$  is pointed if and only if there is a linear functional  $f$  on  $\mathbb{R}^N$  such that  $C' = \{v \in C \mid f(v) = 1\}$  is compact and satisfies  $C = \{\lambda v \mid v \in C', \lambda \geq 0\}$ .*

We proceed the proof of Proposition 11. Put  $N = \dim(\mathcal{S}) < \infty$  and let  $\mathcal{S} \subset V = \mathbb{R}^N$  (recall that now

$\mathcal{S}$  is finite dimensional). Choose  $s_1, \dots, s_{N+1} \in \mathcal{S}$  such that  $V$  is the affine hull of these  $N+1$  points. Then any affine functional on  $\mathcal{S}$  extends to a unique affine functional on  $V$ , therefore the set  $\text{Aff}_{\mathcal{S}}^+$  of all nonnegative affine functionals  $f$  on  $\mathcal{S}$  can be embedded in  $V' = \mathbb{R}^{N+1}$  where the  $i$ -th coordinate signifies the value at  $s_i$ . Now the embedded image of  $\text{Aff}_{\mathcal{S}}^+$  in  $V'$  is a pointed closed convex cone, where the closedness follows since elements  $f$  of the set  $\text{Aff}_{\mathcal{S}}^+$  are characterized by closed relations among the values of  $f$  at the points  $s_i$ . Thus by Lemma 10, there exists a linear functional  $g$  on  $V'$  such that  $C = \{e \in \text{Aff}_{\mathcal{S}}^+ \mid g(e) = 1\}$  is compact and satisfies  $\text{Aff}_{\mathcal{S}}^+ = \{\lambda e \mid e \in C, \lambda \geq 0\}$ . Note that  $C$  is convex by definition.

Let  $0 \neq e \in \mathcal{E}(\mathcal{S})$ . Then we have  $\lambda e \in C$  for some  $\lambda > 0$  by the property of  $C$ . Since  $C$  is compact and convex, the Krein-Milman's Theorem implies that  $\lambda e$  can be written as a finite convex combination  $\lambda e = \sum_x p_x \bar{e}_x$  of extreme points  $\bar{e}_x$  of  $C$ . Since  $\mathcal{S}$  is compact, by taking a sufficiently small  $\mu > 0$  it follows that  $e_x = \mu \bar{e}_x \in \mathcal{E}(\mathcal{S})$  for every  $x$ . Moreover, choose an integer  $k > 0$  such that  $k\lambda\mu \geq 1$ . Then we have a decomposition

$$e = k \sum_x \frac{p_x}{k\lambda\mu} e_x, \quad \frac{p_x}{k\lambda\mu} e_x \in \mathcal{E}(\mathcal{S})$$

of  $e$  into a finite collection of effects (note that  $0 \leq p_x/(k\lambda\mu) \leq 1$ ).

Our remaining task is to show that each  $q_x e_x$ , where  $q_x = p_x/(k\lambda\mu)$ , is an indecomposable effect provided  $q_x > 0$ . Let  $q_x e_x = e' + e''$  with  $e', e'' \in \mathcal{E}(\mathcal{S})$ ,  $e', e'' \neq 0$ . Then we have  $\bar{e}_x = (q_x \mu)^{-1}(e' + e'')$ . By the property of  $C$ , there exist  $\nu', \nu'' > 0$  and  $\bar{e}', \bar{e}'' \in C$  such that  $e' = \nu' \bar{e}'$  and  $e'' = \nu'' \bar{e}''$ . We have  $\bar{e}_x = \eta' \bar{e}' + \eta'' \bar{e}''$ , where  $\eta' = (q_x \mu)^{-1} \nu' > 0$  and  $\eta'' = (q_x \mu)^{-1} \nu'' > 0$ . Moreover, by the definition of  $C$ , we have

$$1 = g(\bar{e}_x) = \eta' g(\bar{e}') + \eta'' g(\bar{e}'') = \eta' + \eta''.$$

Since  $\bar{e}_x$  is an extreme point of  $C$ , it follows that  $\bar{e}_x = \bar{e}' = \bar{e}''$ , therefore  $e' = \nu' \bar{e}_x = (\nu'/(\mu q_x)) q_x e_x$ . Hence  $q_x e_x$  is indecomposable as desired, concluding the proof of Proposition 11. ■

**[Proof of Lemma 2]** It is easy to show  $\tilde{e}$  is an effect. Let  $\tilde{e} = e_1 + e_2$  be an effect decomposition of  $\tilde{e}$ . Then,  $e = qe_1 + qe_2$  is an effect decomposition of  $e$  since  $q \leq 1$ . Since  $e$  is indecomposable, there exists  $c \in \mathbb{R}$  such that  $qe_1 = ce$ , or  $e_1 = c\tilde{e}$ . Thus,  $\tilde{e}$  is indecomposable. ■

**[Proof of Lemma 3]** Let  $e = \lambda e_1 + (1 - \lambda) e_2$  be a convex decomposition of  $e$  with  $\lambda \in (0, 1)$ . It is easy to see that  $e_1(s) = e_2(s) = 1$ . Since  $\lambda e_1, (1 - \lambda) e_2 \in \mathcal{E}$  and  $e$  is indecomposable, we have  $\lambda e_1 = ce$  for some  $c \in \mathbb{R}$ . Applying this to  $s$ , we have  $\lambda = c$ , and thus  $e_1 = e$ . Therefore,  $e$  is a pure effect. ■

**[Proof of Lemma 4]** First we show that an indecomposable  $e$  is not constant on  $\mathcal{S}$ . Since  $\mathcal{S}$  has at least two states, the separation property of states implies that a non-constant effect  $f \in \mathcal{E}(\mathcal{S})$  exists. If  $e$  takes constantly

$c \in (0, 1]$ , then the decomposition  $e = cf + c(u - f)$  contradicts that  $e$  is indecomposable. Hence  $e$  is not constant. Second, if  $e$  does not take 0 at any state, then we have  $e(s) \geq c$  for some  $c > 0$  and all  $s \in \mathcal{S}$  since  $e$  is continuous and  $\mathcal{S}$  is compact. Now the decomposition  $e = cu + (e - cu)$  contradicts that  $e$  is indecomposable. Hence  $e$  takes 0 at some state. ■

**[Proof of Proposition 18]** First we compute  $S_1(s)$  for  $s = (c_1, c_2) \in \mathcal{S}_{\text{sq}}$ . Let  $M = (m_i)_i$  be an indecomposable measurement. To compute  $S_1$ , it suffices to consider the case that  $M$  contains at most one effect  $m_i$  of each of the four types listed in Table I; indeed, if  $m_{i_1}$  and  $m_{i_2}$  are of the same type (i.e.,  $m_{i_2} = \lambda m_{i_1}$  for some  $\lambda \in \mathbb{R}$ ), then by replacing the pair of  $m_{i_1}$  and  $m_{i_2}$  with  $m_{i_1} + m_{i_2}$  the value of  $H(m_i(s))$  is not increased. Thus we may assume without loss of generality that  $M$  consists of the four effects in Table I with parameters  $\alpha_1 = \alpha_2 = \alpha$ ,  $\alpha_3 = \alpha_4 = \beta := 1 - \alpha$  for some  $\alpha \in [0, 1]$ . Now, by putting  $g(x) = -x \log x$  we have

$$\begin{aligned} H(m_i(s)) &= g(\alpha c_1) + g(\alpha(1 - c_1)) + g(\beta c_2) + g(\beta(1 - c_2)) \\ &= g(\alpha) + \alpha h(c_1) + g(\beta) + \beta h(c_2) \\ &= h(\alpha) + \alpha h(c_1) + (1 - \alpha) h(c_2). \end{aligned}$$

Since the right-hand side is concave on  $\alpha \in [0, 1]$ , it takes the minimum at either  $\alpha = 0$  or  $\alpha = 1$ , hence we have  $S_1(s) = \min[h(c_1), h(c_2)]$  as desired.

Second, we compute  $S_2(s)$  for  $s = (c_1, c_2) \in \mathcal{S}_{\text{sq}}$ . Let  $\{p_x, s_x\}_x \in \mathcal{P}(s)$  with  $s_x = (c_{x,1}, c_{x,2})$  and  $M = (m_j)_j \in \mathcal{M}_{\text{ind}}$ . Again, it suffices to consider the case that  $M$  contains at most one effect  $m_j$  of each of the four types listed in Table I; indeed, if  $m_{j_1}$  and  $m_{j_2}$  are of the same type (in the above sense), then by replacing the pair of  $m_{j_1}$  and  $m_{j_2}$  with  $m_{j_1} + m_{j_2}$  the value of  $H(X : J)$  is not changed. Thus we may assume without loss of generality that  $M$  consists of the four effects in Table I with parameters  $\alpha_1 = \alpha_2 = \alpha$ ,  $\alpha_3 = \alpha_4 = \beta := 1 - \alpha$  for some  $\alpha \in [0, 1]$ . Now a direct calculation implies that

$$\begin{aligned} H(X : J) &= h(\alpha) + \alpha h(c_1) + \beta h(c_2) \\ &\quad - \sum_{x \in X} p_x (h(\alpha) + \alpha h(c_{x,1}) + \beta h(c_{x,2})) \\ &= \alpha (h(c_1) - \sum_x p_x h(c_{x,1})) + \beta (h(c_2) - \sum_x p_x h(c_{x,2})). \end{aligned}$$

Since all the pure states  $(c_{x,1}, c_{x,2})$  in  $\mathcal{S}_{\text{sq}}$  satisfy that  $c_{x,1} \in \{0, 1\}$  and  $c_{x,2} \in \{0, 1\}$ , we have  $H(X : J) = \alpha h(c_1) + \beta h(c_2) = \alpha h(c_1) + (1 - \alpha) h(c_2)$ , which is independent of the given decomposition  $\{p_x, s_x\}_x$  of  $s$ . This implies that  $S_2(s) = \sup_{X,J} H(X : J) = \max[h(c_1), h(c_2)]$ , as desired.

Finally, we compute  $S_3(s)$  for  $s = (c_1, c_2) \in \mathcal{S}_{\text{sq}}$ . By the reason similar to the case of  $S_1$ , to compute  $S_3(s)$  it suffices to consider a decomposition  $\{p_x, s_x\}_{x \in X} \in \mathcal{P}(s)$  such that all  $s_x$  are different pure states. Thus we may

assume that  $X = \{00, 01, 10, 11\}$ ,  $s_{00} = (0, 0)$ ,  $s_{01} = (0, 1)$ ,  $s_{10} = (1, 0)$  and  $s_{11} = (1, 1)$ . Now by putting  $p_{11} = p$  we have

$$p_{10} = c_1 - p, p_{01} = c_2 - p, p_{00} = 1 - c_1 - c_2 + p.$$

In the above expression, we have  $p_x \in [0, 1]$  for every  $x$  if and only if  $p_m \leq p \leq p_M$ , where

$$p_m = \max[0, c_1 + c_2 - 1], p_M = \min[c_1, c_2].$$

Hence we have  $S_3(s) = \inf_{p_m \leq p \leq p_M} H(p_x)$ . Now a direct calculation shows that

$$\left(\frac{d}{dp}\right)^2 H(p_x) = - \sum_{x \in X} \frac{1}{p_x} < 0$$

for any  $p \in (p_m, p_M)$ , therefore  $H(p_x)$  takes the minimum at either  $p = p_m$  or  $p = p_M$ :  $S_3(s) = \min[H(p_x)|_{p=p_m}, H(p_x)|_{p=p_M}]$ .

First we consider the case that  $c_1 \leq c_2$  and  $c_1 + c_2 \leq 1$  (i.e.,  $s \in R_{2U}$  or  $s \in R_{2B}$ ), therefore  $p_m = 0$  and  $p_M = c_1$ . If  $p = p_m$  then we have  $(p_x)_x = (1 - c_1 - c_2, c_2, c_1, 0)$ , while if  $p = p_M$  then we have  $(p_x)_x = (1 - c_2, c_2 - c_1, 0, c_1)$ . This implies that

$$\begin{aligned} \text{diff}_{M-m} &:= H(p_x)|_{p=p_M} - H(p_x)|_{p=p_m} \\ &= g(c_2 - c_1) + g(1 - c_2) - g(c_2) - g(1 - c_1 - c_2) \end{aligned}$$

where  $g(a) = -a \log a$ , therefore

$$\frac{\partial}{\partial c_2} \text{diff}_{M-m} = \log \frac{(1 - c_2)c_2}{(c_2 - c_1)(1 - c_1 - c_2)}$$

which is now non-negative by the conditions for  $c_1$  and  $c_2$ . Since  $\text{diff}_{M-m} = 0$  when  $c_2 = 1/2$ , it follows that  $\text{diff}_{M-m} \leq 0$  and  $S_3(s) = H(p_x)|_{p=p_M}$  when  $0 \leq c_2 \leq 1/2$  (i.e.,  $s \in R_{2B}$ ), and  $\text{diff}_{M-m} \geq 0$  and  $S_3(s) = H(p_x)|_{p=p_m}$  when  $1/2 \leq c_2 \leq 1$  (i.e.,  $s \in R_{2U}$ ). Hence the expressions of  $S_3(s)$  in (18) for  $s \in R_{2U}$  and  $s \in R_{2B}$  are proved. The claim for the remaining cases follow by considering suitable symmetry of the state space  $\mathcal{S}_{\text{sq}}$ . ■

**[Proof of Proposition 19]** The first inequality  $S_1(s) \leq S_2(s)$  is obvious by (16) and (17). For the second inequality  $S_2(s) \leq S_3(s)$ , by symmetry, we may assume without loss of generality that  $s = (c_1, c_2) \in R_{2U}$ , i.e.,  $1/2 \leq c_2 \leq 1 - c_1$ . This condition implies that  $h(c_1) \leq h(c_2)$ , therefore  $S_2(s) = h(c_2)$ . On the other hand, (18) implies that  $S_3(s) = g(c_1) + g(c_2) + g(1 - c_1 - c_2)$ , where  $g(x) = -x \log x$ . Thus we have

$$S_3(s) - S_2(s) = g(c_1) + g(1 - c_1 - c_2) - g(1 - c_2)$$

which is a decreasing function of  $c_2$  in this range, while  $S_3(s) - S_2(s) = 0$  when  $c_2 = 1 - c_1$ . This implies that  $S_3(s) \geq S_2(s)$  for any  $s \in R_{2U}$ , hence the claim holds. ■

**[Proof of Lemma 6]** For each  $x \in X$ , let  $\{q_y^x, t_y^x\}_{y \in Y_x} \in \mathcal{D}(s_x)$  and  $M_x = (m_j^x)_{j \in J_x} \in \mathcal{M}$ . Then we have  $\{p_x q_y^x, t_y^x\}_{x \in X, y \in Y_x} \in \mathcal{D}(s)$  and  $M' = (\pi_x m_j^x)_{x \in X, j \in J_x} \in \mathcal{M}$ . Let  $Z = \{(x, y) \mid x \in X, y \in Y_x\}$  and  $K = \{(x, j) \mid$

$x \in X, j \in J_x\}$  denote the index sets of these ensembles, respectively. Then, by putting  $h(a) = -a \log a$  we have

$$\begin{aligned} H(Z : K) &= H(K) - H(K \mid Z) \\ &= \sum_{(x,j) \in K} h(\pi_x m_j^x(s)) - \sum_{\substack{(x',y) \in Z \\ (x,j) \in K}} p_{x'} q_y^{x'} h(\pi_x m_j^x(t_y^{x'})) \\ &= \sum_{(x,j)} m_j^x(s) h(\pi_x) - \sum_{(x',y), (x,j)} p_{x'} q_y^{x'} m_j^x(t_y^{x'}) h(\pi_x) \\ &\quad + \sum_{(x,j)} \pi_x h(m_j^x(s)) - \sum_{(x',y), (x,j)} p_{x'} q_y^{x'} \pi_x h(m_j^x(t_y^{x'})) \\ &= (1 - \sum_{(x',y)} p_{x'} q_y^{x'}) \sum_x h(\pi_x) \\ &\quad + \sum_{(x,j)} \pi_x \left( h(m_j^x(s)) - \sum_{(x',y)} p_{x'} q_y^{x'} h(m_j^x(t_y^{x'})) \right) \\ &= \sum_{(x,j)} \pi_x \left( h(m_j^x(s)) - \sum_{(x',y)} p_{x'} q_y^{x'} h(m_j^x(t_y^{x'})) \right). \end{aligned}$$

Since  $m_j^x(s) = p_x m_j^x(s_x) + \sum_{(x',y) \in Z; x' \neq x} p_{x'} q_y^{x'} m_j^x(t_y^{x'})$  and  $h(a)$  is concave on  $a \in (0, 1)$ , we have  $h(m_j^x(s)) \geq p_x h(m_j^x(s_x)) + \sum_{(x',y); x' \neq x} p_{x'} q_y^{x'} h(m_j^x(t_y^{x'}))$ , therefore

$$\begin{aligned} H(Z : K) &\geq \sum_{(x,j)} \pi_x \left( p_x h(m_j^x(s_x)) - \sum_{y \in Y_x} p_x q_y^x h(m_j^x(t_y^x)) \right) \\ &= \sum_{x \in X} \pi_x p_x H(Y_x : J_x). \end{aligned}$$

By taking the supremum over all  $\{q_y^x, t_y^x\}_{y \in Y_x}$  and  $M_x$ ,  $x \in X$  (see Lemma 5), it follows that

$$S_2(s) \geq \sup H(Z : K) \geq \sum_{x \in X} \pi_x p_x S_2(s_x).$$

Hence Lemma 6 holds. ■

**[Proof of Lemma 7]** We use induction on the number  $N$  of indices  $j$  such that  $x_j \notin \{0, 1/k\}$ . The claim is trivial if  $N = 0$ , while it cannot happen that  $N = 1$ . We assume  $N \geq 2$ , and  $0 < x_1 \leq x_2 < 1/k$  by symmetry. Now if  $x_1 + x_2 \leq 1/k$ , then we have  $h(x_1) + h(x_2) \geq h(x_1 + x_2)$ , therefore  $H(x) \geq H(y)$  where  $y = (x_1 + x_2, x_3, \dots, x_\ell)$ . On the other hand, if  $x_1 + x_2 > 1/k$ , then we have  $h(x_1) + h(x_2) \geq h(x_1 + x_2 - 1/k) + h(1/k)$ , therefore  $H(x) \geq H(y)$  where  $y = (x_1 + x_2 - 1/k, 1/k, x_3, \dots, x_\ell)$ . In any case, we have  $H(y) \geq \log k$  by the induction hypothesis. Hence  $H(x) \geq \log k$  as desired. ■

**[Proof of Lemma 8]** Choose  $t_1, t_2, \dots, t_n \in \mathcal{S}$  ( $n = \dim \mathcal{S} + 1$ ) such that these are affine independent. Then any element  $t$  of  $\mathcal{S}$  has a unique expression  $t = \lambda_1 t_1 + \dots + \lambda_n t_n$ ,  $\sum_j \lambda_j = 1$ . Let  $\varphi : \mathcal{S} \rightarrow \mathbb{R}^n$  denote the map  $t \mapsto (\lambda_1, \dots, \lambda_n)$ . Since  $\mathcal{S}$  is a topological subspace of a finite-dimensional Euclidean space,  $\mathcal{S}$  and  $\varphi(\mathcal{S}) \subset \mathbb{R}^n$  are homeomorphic via  $\varphi$ . By identifying  $\mathcal{S}$  with  $\varphi(\mathcal{S})$  in this

way, the map  $f_s$  is written as  $f_s(e; \lambda_1, \dots, \lambda_n) = \lambda_1 e(t_1) + \dots + \lambda_n e(t_n)$ . This implies that  $f_s$  is continuous, since both  $(e; \lambda_1, \dots, \lambda_n) \mapsto e(t_j)$  and  $(e; \lambda_1, \dots, \lambda_n) \mapsto \lambda_j$  are continuous. ■

## APPENDIX B: GPT WITHOUT COMPLETE MEASUREMENTS.

Here we give an example of a GPT that has no complete measurements. First note that any nonzero extreme effect  $e$  takes 1 at some state, as otherwise we have a nontrivial expression  $e = c(c^{-1}e) + (1 - c)0$  as a convex combination of effects, where  $c = \sup_{s \in \mathcal{S}} e(s) \in (0, 1)$ .

We consider a GPT with state space  $\mathcal{S}$  which is the convex hull of four points  $(0, 0)$ ,  $(1, 0)$ ,  $(0, 1)$ ,  $(2, 2)$  in  $\mathbb{R}^2$ . Then by the above observation and Lemma 4, each indecomposable extreme effect  $e$  takes 0 at an edge of  $\mathcal{S}$

and takes 1 at some state (precisely, at the vertex of  $\mathcal{S}$  farthest from the edge). Thus there are four indecomposable extreme effects in total, as listed in Table II. Now it is obvious that no complete measurements exist in the GPT, since the sum of the values of indecomposable extreme effects at the state  $(0, 0)$  cannot equal to 1.

TABLE II: Indecomposable extreme effects in Appendix B

effect	value at			
	$(0, 0)$	$(1, 0)$	$(0, 1)$	$(2, 2)$
$e_1$	0	0	1/2	1
$e_2$	0	1/2	0	1
$e_3$	2/3	0	1	0
$e_4$	2/3	1	0	0

- 
- [1] G. Mackey, *Mathematical Foundations of Quantum Mechanics* (Dover, 1963).
- [2] S. P. Gudder, *Stochastic Method in Quantum Mechanics* (Dover, 1979).
- [3] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
- [4] G. Ludwig, *Foundations of Quantum Mechanics I, II* (Springer, 1983).
- [5] B. Davies, J. T. Lewis, *Comm. Math. Phys.* **17**, 239 (1970); M. Ozawa, *J. Math. Phys.* **25**, 79 (1984).
- [6] M. Ozawa, *Rep. Math. Phys.* **18**, 11 (1980).
- [7] H. Barnum, J. Barrett, M. Leifer, A. Wilce, *Phys. Rev. Lett.* **99**, 240501 (2007); *ibid*, arXiv:0805.3553.
- [8] J. Barrett, arXiv:quant-ph/0508211.
- [9] A. J. Short, S. Popescu and N. Gisin, *Phys. Rev. A* **73**, 012101 (2006).
- [10] G. M. D'Ariano, arXiv:0807.4383. To appear in "Philosophy of Quantum Information and Entanglement" (Cambridge University Press, Cambridge UK); G. Chiribella, G. M. D'Ariano, P. Perinotti, arXiv:0908.1583.
- [11] G. Kimura, T. Miyadera, H. Imai, *Phys. Rev. A* **79**, 062306 (2009).
- [12] C. Zander, and A. R. Plastino, *EPL*, **86** 18004 (2009).
- [13] K. Nuida, G. Kimura, T. Miyadera, arXiv:0906.5419.
- [14] H. Barnum, et al., arXiv:0805.3553.
- [15] M. Jammer, *The Philosophy of Quantum Mechanics* (John Wiley & Sons Inc, 1974).
- [16] G. Birkhoff, J. von Neumann, *Ann. Math.* **37**, 823 (1936); A. M. Gleason, *J. Math. Mech.* **6**, 885 (1957); C. Piron, *Helv. Phys. Acta*, **37**, 439 (1964); S. Pulmannova, *Int. J. Theor. Phys.* **35**, 2309 (1996).
- [17] P. Jordan, et al., *Ann. Math.* **35**, 29 (1934); I. E. Segal, *Ann. Math.* **48**, 930 (1947).
- [18] C. A. Fuchs, quant-ph/0205039.
- [19] R. Clifton, et al., *Found. Phys.* **33**, 1561 (2003).
- [20] J. Barrett, L. Hardy, A. Kent, *Phys. Rev. Lett.* **95**, 010503 (2005).
- [21] G. Kimura, et al. (in preparation).
- [22] H. H. Schaefer, *Topological Vector Spaces* (2nd edition, Springer, 1999).
- [23] S. R. Lay, *Convex Sets and Their Applications* (Krieger Publishing Company, 1982).
- [24] C. A. Fuchs, J. Graaf, *IEEE Trans. Info. Theory* **45**(4): 1216 (1999).
- [25] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge) 2000.
- [26] C. A. Fuchs and C. M. Caves, *Open Sys. Info. Dyn.* **3**, 345 (1995).
- [27] A. S. Holevo, *Probl. Inform. Transm.* **9**, 110 (1973); H. P. Yuen, M. Ozawa, *Phys. Rev. Lett.* **70**, 363, (1993).
- [28] E. T. Jaynes, *Phys. Rev.* **108**, 171 (1957).
- [29] J. Borwein, A. S. Lewis, *Convex Analysis and Nonlinear Optimization, second edition* (Springer, 2006).
- [30] M. Takesaki, *Theory of Operator Algebra I* (Springer, 1979).
- [31] A. J. Short, S. Wehner, arXiv:0909.4801.
- [32] H. Barnum, et al., arXiv:0909.5075.
- [33] Although the proof is simple (see for instance [7, 30]), this property is important in its applications. For instance, in the context of key distribution, Alice and Bob can assure to be safe if there joint state is pure, since then their system does not have any correlations with another system (eavesdropper).
- [34] Let  $e$  be an effect where  $e(\mathbf{p}^{(i)}) = 1$  or 0 for any  $i$ . Assume that there exists  $f, g \in \mathcal{E}(\mathcal{S}_c)$  and  $\lambda \in (0, 1)$  such that  $e = \lambda f + (1 - \lambda)g$ . Since  $e(\mathbf{p}^{(i)})$  are 1 or 0 and  $\lambda \in (0, 1)$ , one can show  $f(\mathbf{p}^{(i)})$  are also restricted to be 1 or 0. Therefore,  $e = f = g$ , and  $e$  is an extreme point. Next, let  $e$  be an effect where there exists  $i_0$  such that  $e(\mathbf{p}^{(i_0)}) \in (0, 1)$ . Let  $i_m \in \{1, \dots, d\}$  such that  $e(\mathbf{p}^{(i_m)})$  is a minimum value among all  $e(\mathbf{p}^{(i)}) \neq 0$ , i.e.,  $e(\mathbf{p}^{(i)}) \neq 0 \Rightarrow e(\mathbf{p}^{(i)}) \geq e(\mathbf{p}^{(i_m)})$ . Let  $f, g$  be effects defined by  $f(\mathbf{p}^{(i)}) = \delta_{ii_m}$ , i.e.,  $f = e^{(i_m)}$  and  $g(\mathbf{p}^{(i)}) = \frac{x_i - x_{i_m}}{1 - x_{i_m}}$ . It is easy to see  $e \neq f, g$  and  $e = \lambda f + (1 - \lambda)g$  for  $\lambda := e(\mathbf{p}^{(i_m)}) \in (0, 1)$ . Therefore,  $e$  is not an extreme point and this completes the proof. ■
- [35] Let  $\rho = \sum_{j=1}^d \rho_j |\phi_j\rangle\langle\phi_j|$  be an eigenvalue decomposition of  $\rho$ . Notice that  $\{\phi_j\}_{j=1}^d$  is an orthonormal basis of  $\mathcal{H}$



and  $\sum_{j=1}^d |\langle \psi | \rho_j \rangle|^2 = \|\psi\|^2 \leq 1$ . Thus  $(q_j)_{j=1}^{d+1}$  where  $q_j := |\langle \psi | \rho_j \rangle|^2$  ( $j = 1, \dots, d$ ) and  $q_{d+1} := 1 - \sum_j |\langle \psi | \rho_j \rangle|^2$  is a probability distribution. From the concavity of  $f$ , we get

$$f(\langle \psi | \rho | \psi \rangle) = f\left(\sum_{j=1}^{d+1} \rho_j q_j\right) \geq \sum_{j=1}^{d+1} q_j f(\rho_j) = \langle \psi | f(\rho) | \psi \rangle,$$

where  $\rho_{d+1} := 0$ .